



PRIVACY POLICY

Updated August 1st, 2023

GENERAL

In this privacy policy (this “**Policy**”), we describe the personal information that we collect and process about you (provided to us by you or by third parties), the purposes for which we collect and process personal information about you, and the basis on which we collect and process personal information about you, when you use our websites, in connection with the use of our services and/or when we facilitate the processing of your payments on other platforms or websites operated by our clients, when you register for or participate in our webinars or events, if you subscribe to receive news, marketing information or other communications from us, or if you are a prospective customer or user, or if you apply for a job with us.

We recommend that you read this policy carefully in order to understand what Payoneer Inc. and its subsidiaries, including Payoneer Europe Limited, Payoneer Payment Services (UK) Limited, Payoneer Hong Kong Limited and Payoneer Australia Pty Ltd. (“**we**”, “**us**”, “**Payoneer**”) do with your personal information. Your use of our websites and services and any dispute over privacy, is subject to this Policy and any of our applicable Terms and Conditions for use of our services.

Important Notes:

- ADDITIONAL TERMS FOR CUSTOMERS OF PAYONEER EUROPE LIMITED (WHICH INCLUDE EUROPEAN ECONOMIC AREA (“EEA”) AND UNITED KINGDOM (“UK”) RESIDENTS): Please note that the whole of this Policy applies to you, together with additional provisions which are specific to customers of Payoneer Europe Limited and can be found at [Appendix 1](#).
- ADDITIONAL TERMS FOR AUSTRALIAN RESIDENTS ONLY: Please note that the whole of this Policy applies to you together with additional provisions which are specific to Australian residents and can be found at [Appendix 2](#).
- ADDITIONAL TERMS FOR CALIFORNIA RESIDENTS ONLY: Please note that the whole of this Policy applies to you together with additional provisions which are specific to residents of California and can be found at [Appendix 3](#).
- ADDITIONAL TERMS FOR BRAZILIAN RESIDENTS ONLY: Please note that the whole of this Policy applies to you together with additional provisions which are specific to Brazilian residents and can be found at [Appendix 4](#).
- ADDITIONAL TERMS FOR CHINESE RESIDENTS ONLY: Please note that the whole of this Policy applies to you together with additional provisions which are specific to Chinese residents (Mainland China) and can be found at [Appendix 5](#).



- ADDITIONAL TERMS FOR HONG KONG RESIDENTS ONLY: Please note that the whole of this Policy applies to you together with additional provisions which are specific to residents of the Hong Kong Special Administrative Region of the People's Republic of China ("Hong Kong") and can be found at [Appendix 6](#).
- ADDITIONAL TERMS FOR JAPANESE RESIDENTS ONLY: Please note that the whole of this Policy applies to you together with additional provisions which are specific to Japanese customers of Payoneer Inc. and can be found at [Appendix 7](#). Kindly note however, that this Privacy Policy does not apply to our customers in Japan who have subscribed to a Payoneer Card. If you are a holder of a Payoneer Card in Japan please review your applicable Policy [here](#).
- ADDITIONAL TERMS FOR SOUTH AFRICAN RESIDENTS ONLY: Please note that the whole of this Policy applies to you together with additional provisions which are specific to South African residents and can be found at [Appendix 8](#).
- ADDITIONAL TERMS FOR SINGAPORE RESIDENTS ONLY: Please note that the whole of this Policy applies to you together with additional provisions which are specific to Singapore residents and can be found at [Appendix 9](#).
- ADDITIONAL TERMS FOR REPUBLIC OF KOREA RESIDENTS ONLY: Please note that the whole of this Policy applies to you together with additional provisions which are specific to Republic of Korea residents and can be found at [Appendix 10](#).
- ADDITIONAL TERMS FOR UK RESIDENTS ONLY: Please note that the whole of this Policy applies to you, together with additional provisions which are specific to residents of the United Kingdom can be found at [Appendix 11](#).

You can find a copy of this Privacy Policy in PDF format [here](#).

HOW, WHEN, AND WHAT WE COLLECT?

How does Payoneer collect my personal information?

We collect personal information directly from you, about you from third parties such as our marketing affiliates and service providers used to verify your identity and prevent fraudulent activity, other Payoneer users and other Payoneer clients or customers, for the purpose of providing our services to you or to facilitate the processing of your payments on other platforms or websites operated by our users, or as part of a customer referral program, and automatically as you use our websites and/or our services.

When does Payoneer collect my personal information?

- When you apply for and use any of our services, when we facilitate the processing of your payments on other platforms or websites operated by our users, when you



contact us with questions, and when you otherwise choose to provide personal information to us.

- We receive personal information about you from banking references, credit reporting agencies, affiliates, other Payoneer users, and other third parties (e.g., entities that assist us in validating your identity, for risk assessment purposes, for fraud prevention, etc.). We combine this information with other information that we collect about you.
- We, and our third party service providers, automatically collect the following information about your use of our websites and/or our services through cookies, web beacons, log files and other technologies (subject to your consent where required by applicable law): your domain name, your browser type and operating system, web pages you view, links you click, your IP address, the length of time you visit our websites and/or use our services, your activities on our websites, and the referring URL or the webpage that led you to our websites.
- If you are a registered user using our mobile application, we also collect the following information about you: mobile device ID; device name and model; operating system type, name, and version; your activities within the mobile application, the length of time that you are logged into our mobile application, and, with your permission, your geo-location information. Please see our [Cookies Policy](#) for more information.
- When you register an account with the Payoneer Affiliates performance marketing partner network.
- When you provide services to Payoneer as a representative of a third party that Payoneer has engaged.
- When you apply for a job with Payoneer, we may collect personal information from you or from a third party such as a recruiter or verification services provider.

What personal information does Payoneer collect?

The types of personal information we collect about you depends on your particular interaction with our websites and/or how you use our services, including when we facilitate the processing of your payments on other platforms or websites operated by our users. This may include, where permitted by applicable law and as relevant for your use of the services:

Categories of Personal Information Collected	Specific Personal Information	Source of Personal Information
Identifiers	Name, email address, phone number, billing or mailing address, date of birth, national identification numbers and documents that may include your photograph.	Directly from you, third parties on your behalf and as instructed by you, other Payoneer users and customers, our service providers and affiliates.
Financial Information	Bank and credit account information, credit history as	Directly from you, third parties on your behalf



	applicable, details of any transactions carried out using any of our services.	and as instructed by you, other Payoneer users and customers, our service providers and affiliates.
Internet or Other Similiar Network Activity; Device Information	<p>Your interaction with our websites, internet protocol (IP) address, browser type and version, cellular network, operating system.</p> <p>Other information collected through Cookies and other tracking technologies as listed above and as described in our Cookies Policy</p>	From you directly and our third party analytic tools and cookies usage (See our Cookies Policy for more information).
Commercial Information	Information about your business.	Directly from you, third parties on your behalf and as instructed by you, other Payoneer users and customers, our service providers and affiliates.
Geolocation Data	Geolocation.	Directly from you and/or through your use of the mobile application and/or our third party analytic tools and cookies usage (See our Cookies Policy for more information).
Professional or Employment Information (for Job Candidates)	Name and contact information, professional credentials and skills, educational and work history, salary, evaluations, references, interviews, certifications, disciplinary matters and other information of the type included on a resume, curriculum vitae or cover letter.	Directly from you or when another party, such as a recruiter or external website, provides it to us.
Other categories	Any other information that you choose to provide to us (e.g., when you send us an email/otherwise contact us or when you choose to participate	Directly from you, third parties on your behalf and as instructed by you.



	in surveys where you provide feedback on our services). Calls/emails/other correspondence.	
Special categories of Personal Data	Biometric Data in the form of 'selfies' (<i>self-photographs</i>) processed for the purposes of identity verification when you become a customer.	Directly from you, third parties on your behalf and as instructed by you, or from our service providers.

You are responsible for providing accurate and up-to-date information. If you choose to participate in our Refer a Friend program, you acknowledge that you have the right and are duly authorized to provide us with your friend's personal information.

HOW AND WHY WE USE YOUR INFORMATION?

- To validate your identity (including via SMS or Voice Call, as applicable) and verify your access and control over bank accounts you associate with our services.
- To register you and provide our various services to you, to facilitate the processing of your payments on other platforms or websites operated by our users, to communicate with you in connection with our various services and KYC verification processes (including via SMS, messaging applications, or, for users of our Mobile Application, via "push" notifications) or any changes in our Terms and Conditions or this Policy that apply to you.
- For the purpose for which you specifically provide the personal information to us, including, to respond to your inquiries, to provide any information that you request, and to provide customer support (including via SMS, messaging applications, as applicable).
- To tailor the content and information that we send or display to you, to offer location customization (where permitted by applicable law), personalized help and instructions, and to otherwise personalize your experiences while using our websites and/or our services, such as developing and offering you with new and/or additional services to the services we are providing you or new and/or additional features to existing services, based, where appropriate, on your eligibility for such new and/or additional services or features, as would be evaluated by us from time to time.
- For marketing and promotional purposes. For example, we use your email address, phone number (including via SMS, messaging applications, as applicable), and/or mailing address to send you newsletters, special offers and promotions, in connection with your registration to webinars and other events, or to otherwise contact you about services or information we believe will interest you (unless you are opted-out from our marketing communications or you have not opted-in to receiving such communications, as applicable), or to conduct draws for campaigns and the like and deliver prizes and rewards to you.
- As permitted by applicable law, to assist us in advertising our products and services in various mediums including, without limitation, sending you promotional emails,



advertising our services on third party sites and social media platforms, sending you direct mail and by telemarketing (unless you are opted-out from our marketing communications or you have not opted-in to receiving such communications, as applicable).

- To better understand how users, access and use our websites and/or our services, both on an aggregated and individualized basis, to administer, monitor, and improve our websites and/or services, for our internal purposes, and for other research and analytical purposes (including in the form of our online surveys). Please see our [Cookies Policy](#) for more information.
- To protect us, our customers, employees, partners or property — for instance, to investigate fraud and prevent fraudulent activity, abuse of the services, harassment or other types of unlawful activities involving us or other companies that we do business with, to enforce this Policy, as well as our Terms and Conditions.
- We process personal data, such as information submitted to us in a job application, to facilitate our recruitment activities and process employment applications, such as evaluating a job candidate for a position with us and communicating with you regarding your application and future opportunities.

WHEN DO WE DISCLOSE YOUR INFORMATION?

We disclose your personal information to third parties, including service providers, regulated institutions (e.g., financial institutions), affiliated entities, and business partners as set out in the table below. In the table below, we also list the reasons why we disclose information.

How and Why We Disclose Your Information	Does Payoneer Disclose?
With our service providers and affiliates – for our business purposes, such as to assist us with the provision of our services and to verify your identity, prevent, detect and protect against fraudulent activity or abuse of our services, conduct internal research and analytical assessments, process your transactions, maintain your account(s) and provide you with customer care services. These include internet service providers, data and cyber security services, banks, financial institutions, payment processors, financial services providers, remote access services; service providers that help us verify your identity and help us comply with our legal and regulatory obligations, including open-banking service providers; service providers we use to provide customer support (including chatbots); and our business, legal, tax, financial and other advisors, on a confidential basis. Such service providers differ based on the services provided to you and your jurisdiction.	Yes



<p>With fraud prevention and detection service providers – which provide fraud prevention, detection, protection services, or other similar services, on our, or our service provider’s, behalf. Such service providers keep records of information provided and use it when providing fraud detection and prevention services to other users of their databases.</p>	Yes
<p>For marketing purposes:</p> <ol style="list-style-type: none">1. With our service providers and our affiliates – to market our own products and services and for audience creation; and2. With non-affiliated third parties for joint marketing purposes.	Yes
<p>With Payoneer clients, customers or third parties using our services – to perform our services, assist in carrying out your transactions with such clients, customers or third parties or for purposes of our refer-a-friend program(s). In addition, where a Payoneer card is issued to you as an expense card under a Corporate Client expense card program (in accordance with our Terms and Conditions) – we will disclose information related to usage and balance of the card to such corporate client.</p>	Yes
<p>In response to legal process – to comply with the law, a judicial proceeding, subpoena, court order, or other legal process.</p>	Yes
<p>In connection with business transfers – to another entity if we are acquired by or merged with such other entity, if substantially all of our assets are transferred to such other entity, or as part of a bankruptcy proceeding.</p>	Yes
<p>To protect the rights, property, or safety of us and others – we disclose personal information to our business partners, service providers and other third parties when we believe it is necessary or appropriate. This includes exchanging and/or jointly using information with other companies, businesses and organizations when you use our services in connection with such third parties’ or their affiliates’ services and/or when we facilitate the processing of your payments on other platforms or websites operated by our users, for the purpose of us and/or them investigating, preventing, or taking actions regarding suspicious or high risk transactions, illegal activities, suspected fraud or fraudulent operations connected to such other entities’ businesses and/or our services, situations involving potential threats to the safety of any person, violations of our or their Terms and Conditions or this Policy, or as</p>	Yes



evidence in or otherwise connected to litigation in which we or they are involved.	
Aggregated and de-identified information – we disclose aggregate or de-identified information about users for marketing, advertising, research, or similar purposes.	Yes
With consumer reporting agencies, as permitted by law, with respect to users from the United States.	Yes
As a participant in Amazon’s Payment Service Provider Program, designed to enhance its ability to detect, prevent and take action against bad actors, so that Amazon and participating PSPs can continue to protect customers and sellers from fraud and abuse, if your Payoneer account is registered with Amazon, we would disclose to them certain data collected during the account sign-up process and as you use our services. This includes, as applicable, “Know Your Client” data such as identity data (e.g., name, nationality), contact information (e.g., address) and details regarding your accounts with Payoneer and your bank account(s). If your Amazon account is deactivated or terminated by Amazon due to abuse, fraud or illegal activity, we may disclose additional information, including limited transaction related information. Please see Amazon’s PSPP Policy Help page for important details here .	Yes
With our service providers – for their machine-learning algorithms. These service providers use the data we provide to maintain and improve their machine-learning algorithms which they use to provide services to us and to their other clients. When these service providers use data this way their use is subject to their own privacy policies. A list of the service providers which use data for their machine-learning algorithms can be viewed at https://www.payoneer.com/legal/ .	Yes
When you register for an account on the Payoneer Affiliates performance marketing partner network, we use a third-party portal to store your personal information, and we may disclose your personal information with such third party as necessary for the performance of your Payoneer Affiliates performance marketing partner network account. We may also, from time to time, provide such information to certain third-party administrative vendors for efficiency in providing administrative or program management services in connection with your Payoneer Affiliates performance marketing partner network Account.	Yes



If you do not want us to use your details for marketing purposes, and/or to pass your details on to third parties for joint marketing purposes, please contact us through the various communication channels available, as listed under the Section titled [“CONTACT US, QUESTIONS, UPDATING YOUR INFORMATION, OPTING OUT”](#) below. You will also be able to unsubscribe from any marketing emails sent to you by Payoneer using a link provided in such emails.

If you do not want us to disclose your details to our service providers for their machine-learning algorithm purposes, please contact us through the various communication channels available, as listed under the Section titled [“CONTACT US, QUESTIONS, UPDATING YOUR INFORMATION, OPTING OUT”](#) below.

WHERE DO WE STORE YOUR DATA?

All information you provide to us is stored on our secure servers or our third-party cloud service providers. Any payment transactions will be encrypted using SSL technology. Where we have given you (or where you have chosen) a password which enables you to access certain parts of our site, you are responsible for keeping this password confidential. We ask you not to share your password with anyone.

Unfortunately, the transmission of information via the internet is not completely secure. Although we will do our best to protect your personal data, we cannot guarantee the security of your data transmitted to our websites; any transmission is at your own risk. Once we have received your information, we will use strict procedures and security features to try to prevent unauthorized access.

CHANGES TO OUR PRIVACY POLICY

We keep this Policy under regular review and update it from time to time. You will be notified of changes to this Policy via the posting of an updated version on our websites and, where appropriate, via email and/or message to “Payoneer Account”. Changes will take effect upon the date on which an updated Policy is posted on our websites. We recommend that you regularly check for updates or changes to our Policy and that you review this Policy when visiting our websites. We will not materially reduce your rights under this Policy without taking steps to bring such changes to your attention.

CONTACT US, QUESTIONS, UPDATING YOUR INFORMATION, OPTING OUT

If you are a Payoneer customer and would like to update your personal information, please log into your “Payoneer Account” in order to update certain information or contact us through



the contact information below. If you are not a Payoneer customer but have provided us with personal information or if your personal information was provided to us by third parties, and you would like to update your personal information, you may contact us through the phone number or email address listed below. From time to time, we may email you or otherwise contact you with special offers; you can opt-out of those offers by using either the Notification Settings page in "Payoneer Account", the unsubscribe link provided in the email, or by contacting us as noted below.

Payoneer Customer Care:

Payoneer Inc.

150 West 30th Street, Suite 600,

New York, NY, 10001

Phone: 1-800-251-2521 (within the USA) or 1-646-658-3695 (outside the USA)

Email: [Email us](#)

Web: www.payoneer.com

For Payoneer Europe Limited Customers:

Payoneer Europe Limited

6th floor, 2 Grand Canal Square

Dublin 2, D02 A342, Ireland

Email: [Email us](#)

Web: www.payoneer.com

For Payoneer Payment Services (UK) Limited Customers:

Payoneer Payment Services (UK) Limited

37 Broadhurst Gardens

London, England, NW6 3QT

Email: [Email us](#)

Web: www.payoneer.com

For Payoneer Australia Pty Ltd Customers:

Payoneer Australia Pty Ltd

c/ MAZARS (NSW) PTY LIMITED

L 12 90 Arthur Street North Sydney

NSW 2060 Australia



Email: [Email us](#)

Web: www.payoneer.com/au/

Privacy Matters:

- For requests related to deleting your personal data or receiving a copy of your personal data, you can contact us at any time by using this [online form](#).
- For additional queries related to privacy and personal data you can contact our Data Protection Officer at DPO@payoneer.com.

GOVERNING LAW AND JURISDICTION

To the extent required by applicable laws or regulations, this Policy shall be exclusively governed by and interpreted in accordance with the laws of the State of Delaware, and any dispute hereunder shall be brought exclusively in the courts of the State of Delaware except where prohibited by US law.

Notwithstanding the above, for our Australian customers only, this Policy shall be governed by and interpreted in accordance with the laws of Victoria, Australia, and any dispute hereunder shall be brought exclusively in the courts of Victoria.

DATA RETENTION

We retain your personal data for at least such period required in order to meet our obligations under applicable laws or regulations and, to the extent not prohibited under applicable law, such additional period in accordance with our internal policies and procedures for purposes of prevention of fraudulent activities, risk management and security.

DISCLAIMER

Any and all content provided on our websites in relation to our services or otherwise, including links to other websites is provided for information purposes only and does not constitute advice, recommendation or support of such content or website. Payoneer makes every effort to provide true and accurate content on its websites. However, Payoneer provides no warranty, express or implied, of the accuracy, completeness, timeliness, or applicability of such content. Payoneer accepts no responsibility for and excludes all liability in connection with information provided on the Payoneer websites, including but not limited to any liability for errors, inaccuracies or omissions.



APPENDIX 1: ADDITIONAL TERMS FOR PAYONEER EUROPE LIMITED CUSTOMERS

The information below is required pursuant to EEA law regarding privacy and data protection. The terms below apply to Payoneer Europe Limited customers (which include our EEA customers and websites visitors), in addition to the terms in the rest of the Policy.

For the purposes of the General Data Protection Regulation (“GDPR”), the data controller is Payoneer Europe Limited of 6th floor, 2 Grand Canal Square Dublin 2, D02 A342 Ireland, a company established in Ireland and regulated for data protection purposes by the Data Protection Commission (DPC) of Ireland. If you have any questions about this Policy, please contact our Data Protection Officer (DPO) at DPO@payoneer.com.

If you are unhappy about how we are processing your data or how we have responded to a request or complaint, you have the right to make a complaint to the Data Protection Commission (DPC) of Ireland or your local supervisory authority. You can find more details about how to contact the Data Protection Commission (DPC) of Ireland on their [website](#).

WHEN DO WE DISCLOSE YOUR PERSONAL INFORMATION?

The table headed “*How and Why We Disclose Your Information*” in the main part of the Policy under the heading “[WHEN DO WE DISCLOSE YOUR INFORMATION?](#)” lists who we may disclose your information to, which include transfers for reasons of legal compliance and necessity in order to provide you with our services.

You should be aware that when you disclose your information, it will be transferred to, and stored in, countries outside the EEA, as applicable, including the USA and Israel.

Please note that where data is transferred outside of the EEA, these countries may not offer the same level of protection for personal data as is available in the EEA. Payoneer will take various measures to ensure that your data is treated securely, which may include, but not be limited to:

- assessing the security measures taken at any place your personal data is transferred to;
- having suitable contract terms in place that oblige a data processor to only process in accordance with our instructions;
- having monitoring, reporting and resolution procedures in place with regard to ongoing security; and
- only transferring your data via an appropriate safeguard as described in Article 46 of GDPR, including [Standard Contractual Clauses](#) adopted by the European Commission (Article 46.2).

The State of Israel has been assessed by the European Commission as offering an adequate level of data protection and a copy of the adequacy decision is available [here](#).

Please contact us at DPO@payoneer.com if you require more detailed information about international transfers of your personal information, and the safeguards applied.



LEGAL BASES FOR PROCESSING YOUR PERSONAL DATA

We process your personal information based on the following legal bases, as recognised by and in compliance with the applicable data protection laws:

- the processing is necessary to perform our contract with you (i.e., the Terms and Conditions that apply as applicable with respect to our services, for the provision of our services), or to take steps requested by you before entering into said contract;
 - you are obliged to provide us with personal data as it is necessary to enter into and perform our contractual agreements. In the event that you do not wish to provide us with your personal data for the purposes outlined above in the "[HOW AND WHY WE USE YOUR INFORMATION?](#)" section, we will not be able to perform our contractual agreement with you;
- the processing is in Payoneer's or someone else's legitimate interests, and these interests are not overridden by your interests or rights in the protection of your personal data. This may include processing your data for identification or prevention of suspicious or high risk transactions or fraudulent activity, internal research and analytics assessments, for purposes of communication with you, and informing you about new products and services we are offering or to promote new products and services of other parties which we think may be of interest to you, etc.;;
 - before we process your personal data to pursue our legitimate interests for the purposes outlined above in the "[HOW AND WHY WE USE YOUR INFORMATION?](#)" section, we determine if such processing is necessary and we carefully consider the impact of our processing activities on your fundamental rights and freedoms. On balance, we have determined that such processing is necessary for our legitimate interests and that the processing which we conduct does not adversely impact on these rights and freedoms.
- you have given your consent to the processing of your data;
- the processing is necessary to meet a legal obligation which applies to Payoneer.

Sometimes we process data about you which the law considers to fall within special categories (see section "[HOW, WHEN AND WHAT WE COLLECT?](#)" for more details), in which case, we use one of the following grounds:

- the processing is necessary for the establishment, exercise or defence of legal claims;
- you have freely given your informed, specific consent to the processing; or
- the processing is necessary for reasons of substantial public interest, based on applicable law.

If you would like more information about the legal grounds used to process your information, or about the legitimate interests referred to above, please contact us.



In cases where we have asked for, and you have given, your consent to our processing of your personal data, you have the right to withdraw such consent at any time. You can do this by contacting our DPO at DPO@payoneer.com.

DO YOU HAVE TO GIVE US YOUR PERSONAL INFORMATION?

In most cases, providing your personal data to us is optional, however, if you do not provide it, you will not be able to use our services. For example, we need details such as your name, address and bank account details so that we can make payments to you and receive payments from you. In other cases, you have a choice over whether we collect your personal data, for example, you can turn off cookies on your browser and we will not place any cookies on your device or computer (although in this case you may not be able to use all parts of our websites).

PROFILING AND AUTOMATED DECISION MAKING

We may use automated decision making as part of our process to evaluate eligibility for the use of our services. Such decision-making processes are solely automated and do not require human intervention. We use these tools as a measure of fraud prevention and for the purposes of security and risk assessment relating to the performance of our services, to comply with applicable "Anti Money Laundering" (**AML**) and "Know Your Customer" (**KYC**) rules and to verify your identity when you become a customer, including for example:

- (i) Automated tools incorporated in our process of approval of your registration application: based on the information you provide, the tool may advise if additional information is required for purpose of approval of your application.
- (ii) Automated tools incorporated in our process of approval of certain payment transaction of registered users: such tools may advise if additional information is required for purpose of performance of the payment transaction.
- (iii) Automated tools used to verify your identity to enable us to comply with AML and KYC rules applicable to us as a financial services provider. For example, we carry out this process using selfies (*self-photographs*) and other forms of ID when you register to open an account with us and may also use tools that scan documents for authenticity, classify documents into types, extract required information from the document, approve or decline the sufficiency of documents you submit and determine if additional information or documents are required.

You have certain rights in respect of automated decision making, where the decision taken has significant effects on you, as detailed below in the "[YOUR RIGHTS UNDER GDPR](#)" section.

HOW LONG DO WE KEEP YOUR PERSONAL INFORMATION?



Payoneer retains your personal data for the duration of your engagement with us and for a period following termination of your engagement with us, as required by applicable laws or regulations and/or in accordance with Payoneer's internal policies and procedures for purposes of prevention of fraudulent activity, risk management and security. Payoneer will periodically review the necessity of retention of your personal data.

YOUR RIGHTS UNDER GDPR

You have several rights in relation to your personal data which are described in more detail below. You can exercise your rights at any time.

For requests related to deleting your personal data or receiving a copy of your personal data, you can contact us at any time by using this [online form](#).

For additional queries related to privacy and personal data you can contact our Data Protection Officer at DPO@payoneer.com.

Accessing your data

You can ask us to:

- Confirm whether we are processing your personal data.
- Give you a copy of that personal data.
- Provide you with other information about your personal data such as what data we have, what we use it for, who we disclose it to, whether we transfer it outside of the EEA and how we protect it, how long we keep it for, what rights you have, how you can make a complaint, where we got your data from and whether we carry out any automated decision making or profiling. We aim to give you all this information in this Policy, although if anything is unclear, please contact our Data Protection Officer at DPO@payoneer.com.

You do not have to pay a fee for a copy of your personal information unless your request is unfounded, respective or excessive, in which case we will charge a reasonable amount in the circumstances. We will let you know of any charges before completing your request.

Correcting your personal data

You can ask us to correct any personal data which is inaccurate or incomplete. This is free of charge.

If we have disclosed the personal data to anyone else, we will tell them about the correction wherever possible.

If we cannot action a request to correct your personal data, we will let you know and explain why this is.

Erasing your personal data



This right is sometimes referred to as "the right to be forgotten". This is not an absolute right but you have the right to have your data erased, free of charge, in certain circumstances.

You can ask for your personal data to be erased where:

- it is no longer necessary for the purpose for which it was originally collected or processed;
- we are processing your personal data based on your consent, and you withdraw that consent;
- you object to the processing and we do not have an overriding legitimate interest for continuing;
- your personal data has been unlawfully processed;
- your personal data must be erased to comply with a legal obligation;
- the personal data was processed to offer information society services to a child.

There are some exceptions to this right. If one of these applies, we do not have to delete the personal data.

If we have disclosed your personal data to third parties, we will tell them about the erasure of your data unless this is impossible or would involve disproportionate effort.

Please note, in connection with such requests, that personal data may be either deleted or retained in an aggregated manner without being linked to any identifiers or personal data, depending on technical commercial capability.

Restricting the processing of your personal data

You can ask us to restrict the processing of your personal data in some circumstances, free of charge. This is not an absolute right. If processing is restricted we can store the personal data and retain enough information to make sure the restriction is respected unless you consent or the processing is necessary in relation to a legal claim or to protect the rights of another person or for reasons of important public interest, but we cannot further process your personal data.

You can restrict the processing of your personal data in the following cases:

- if you contest the accuracy of your personal data, we will restrict processing until we have made sure the personal data is accurate;
- if you object to our processing pending the verification of whether or not our legitimate interests override your interests, rights and freedoms or in connection with legal proceedings;
- if the processing is unlawful but you do not want us to erase your personal data;



- if we no longer need the personal data but you require the data to establish, exercise or defend a legal claim.

If we have disclosed the data to a third party, we will inform them about the restriction unless it is impossible or would require a disproportionate effort. We will tell you if we decide to lift a restriction on processing your personal data.

Objecting to the processing of your personal data

You have a right to object to the processing of your personal data at any time. This request will be free of charge. It is not an absolute right, but you can object to our processing of your personal data where it is:

- based on the legitimate interest ground; or
- for the purposes of scientific/historical research and statistics.

We will stop processing your personal data unless we have compelling legitimate grounds for the processing which override your interests and rights, or unless we are processing the personal data for the establishment, exercise or defence of legal claims.

You can require us to stop using your personal data for direct marketing purposes. We will stop as soon as we receive your request. There are no exemptions or reasons for us to refuse.

Data Portability

This allows you to obtain and reuse your personal data for your own purposes across different services. It applies where the following conditions are met:

- you provided the personal data to us yourself;
- we are processing the personal data either based on your consent or because it is necessary for the performance of a contract; and
- the processing is carried out by automated means.

We will provide your personal data free of charge in a structured, commonly used and machine-readable form.

Automated decision making and profiling

You have the right not to be subject to a decision which is based solely on automated processing and which produces a legal (or similarly significant) effect on you. In certain circumstances where automated decision making is used, you will be provided with an opt-out option by way of an alternative means of processing.

We will tell you about any automated decision making that affects you. You have the right to:

- request human intervention;
- express your point of view; and



- challenge the decision.

These rights are not absolute. We may not be able to comply with your request to obtain human intervention, obtain your point of view or to contest a decision, if the processing of personal data is:

- necessary for us to enter into or perform a contract with you;
- authorised by law (e.g., for fraud prevention) and which also lays down suitable measures to safeguard your right, freedoms and legitimate interests; or
- based on your explicit consent.

Dealing with requests to exercise your rights

We will respond to your request without undue delay at the latest within one (1) month of receiving your request unless it is particularly complicated or you have made several requests, in which case we may extend this by two (2) months. We will let you know if we are going to take longer than one (1) month in dealing with your request. If we have a lot of information about you we might ask you if you can tell us what exactly you want to receive. This will help us action your request more quickly.

For the purpose of complying with your requests to exercise the rights listed above, we shall perform the necessary internal processes to identify you.



APPENDIX 2: ADDITIONAL TERMS FOR AUSTRALIAN RESIDENTS

We are bound by the Australian Privacy Principles under the Privacy Act 1988 (Cth) and other laws that govern the handling of personal information. The terms below apply to Australian customers in addition to the terms in the rest of the Policy.

We may also disclose such information as required or permitted by any law, for example to meet our obligations under the Anti-Money Laundering and Counter Terrorism Financing Act 2006 (Cth).

You may request to access or correct any personal information we hold about you. We will provide our reasons if we deny any request for access to or correction of personal information. Where we decide not to make a requested correction to your personal information, and you disagree, you may ask us to make a note of your requested correction with the information.

You should be aware that when you disclose your information, it may be transferred to, and stored at, a destination outside Australia including but not limited to the United States of America.

Please note that where data is transferred outside of Australia, other countries may not offer the same level of protection for personal data as is available in Australia under the Privacy Act 1988 (Cth). Nonetheless, Payoneer will take various measures to ensure that your data is treated securely, which may include, but not be limited to:

- assessing the security measures taken at any place your data is transferred to;
- having suitable contract terms in place that oblige a data processor to only process in accordance with our instructions; and
- having monitoring, reporting and resolution procedures in place with regard to ongoing security.

We may also collect, hold, use and disclose certain credit-related personal information about you which may include:

- permitted identification information, e.g., names, date of birth, sex, 3 most recent addresses, employer and driver's licence number;
- your applications for credit - the fact that you have applied for credit and the amount and type of credit;
- the identity of your current and previous credit providers;
- records of previous requests made by credit providers to credit reporting bodies ("CRBs") for information about you in connection with consumer or commercial credit applications, guarantees and securitisation arrangements;



- information about defaults (where repayments are more than 60 days overdue, in certain circumstances);
- where those default repayments are no longer overdue, or new payment arrangements have been agreed;
- a credit provider's opinion that you have committed a serious credit infringement (that is, acted fraudulently or shown an intention not to comply with your credit obligations);
- the start and end dates, credit limits and certain terms and conditions of your credit arrangements;
- information about court judgments against you;
- publicly available information relevant to your credit worthiness;
- certain insolvency information from the National Personal Insolvency Index;
- information derived by CRBs from the above information (e.g., assessments and ratings in respect of your credit worthiness); and
- information we derive from the above information (e.g., our own assessments and ratings in respect of your credit worthiness), ("credit-related personal information").

This may also include information about your arrangements with other credit providers as well as with us.

We may disclose some of these types of information to CRBs. CRBs may use credit-related personal information to maintain records on individuals which they may disclose to other credit providers for those providers' own credit assessments.

We will notify you of the CRBs that we use.

We may also be required to check the validity of your identification documents with the Australia Document Verification Service (DVS).

Where you express any concerns that we have interfered with your privacy or conducted ourselves inconsistently with this Policy, we will respond to let you know who will be handling your matter and when you can expect a further response. We aim to resolve your concerns in a fair and efficient manner within 30 days.

If you are unhappy about how we are processing your data or how we have responded to a request or complaint, you have the right to make a complaint to the Office of the Australian Information Commissioner (OAIC). You can find more details about how to contact the OAIC in writing as set out below:

Website: <https://www.oaic.gov.au/>
Address: GPO Box 5218 Sydney NSW 2001
Fax: +61 2 9284 9666



Email: enquiries@oaic.gov.au



APPENDIX 3: ADDITIONAL TERMS FOR STATE OF CALIFORNIA RESIDENTS

The information below is required under the California Consumer Privacy Act of 2018 (as amended, including by the California Privacy Rights Act of 2020 and the California Consumer Privacy Act Regulations, each as amended (together, the "CCPA")). The terms below apply to residents in the State of California in addition to the terms in the rest of the Policy. These terms below do not address or apply to our handling of personal information that is exempt under the CCPA.

INFORMATION COLLECTION, USE AND DISCLOSURE

Categories of Personal Information Collected and Disclosed

While our processing of personal information varies based upon our relationship and interactions with you, we describe generally, the categories of personal information (as defined by the CCPA) that we have collected about California residents, as well as the categories of third parties to whom we may disclose that information for a business or commercial purpose above under ["HOW, WHEN AND WHAT WE COLLECT?"](#) and ["How and Why We Disclose Your Information"](#) in the main part of the Policy under the heading ["WHEN DO WE DISCLOSE YOUR INFORMATION?"](#).

In addition, where we use, disclose or process de-identified data (data that is no longer reasonably linked or linkable to an identified or identifiable natural person, household, or personal or household device) we will maintain and use the information in de-identified form and not attempt to re-identify the information, except in order to determine whether our de-identification processes are reasonable and adequate pursuant to applicable privacy laws.

Sources of Personal Information

In general, we may collect personal information directly from you, from other customers and users of our services, from advertising networks and from providers of data analytics.

Purposes of Collection, Use and Disclosure

As described in more detail above under ["How and Why We Disclose Your Information"](#) in the main part of the Policy under the heading ["WHEN DO WE DISCLOSE YOUR INFORMATION?"](#), we collect, use, disclose and otherwise process personal information for the following business and commercial purposes and as otherwise directed by you:

- Services and support.
- Analytics and improvement.
- Customization and personalization.
- Marketing and advertising.
- Planning and managing events.



- Research and surveys.
- Security and protection of rights.
- Legal proceedings and obligations.
- To process job applications.
- In support of business transfers (e.g., if we are acquired by another company).

Notwithstanding the above, we only use and disclose sensitive personal information as reasonably necessary (i) to perform our services requested by you, (ii) to help ensure security and integrity, including to prevent, detect, and investigate security incidents, (iii) to detect, prevent and respond to malicious, fraudulent, deceptive, or illegal conduct, (iv) to verify or maintain the quality and safety of our services, (v) for compliance with our legal obligations, (vi) to our service providers who perform services on our behalf, and (vii) for purposes other than inferring characteristics about you. We do not use or disclose your sensitive personal information other than as authorized by the CCPA.

Retention

We retain your personal information for at least such period required in order to meet our obligations under applicable laws or regulations and, to the extent not prohibited under applicable law, such additional period in accordance with our internal policies and procedures for purposes of prevention of fraudulent activities, risk management and security.

CCPA REQUESTS

Under the CCPA residents in the State of California are provided with specific rights regarding the collection, use and disclosure of their personal information subject to certain limitations and exemptions.

CCPA Information Request Rights

You or your authorized agent may apply to us with requests as detailed below by contacting us through phone: 1-800-251-2521 (within the USA) or through the [online form](#) on our websites.

We will take steps to verify your request by matching the information provided by you with the information we have in our records. You must complete all required fields on our webform to verify your request. We will process your request based upon the personal information in our records that is linked or reasonably linkable to the information provided in your request. In some cases, we may request additional information in order to verify your request or where necessary to process your request. If we are unable to adequately verify a request, we will notify the requestor. Authorized agents may initiate a request on behalf of another individual; authorized agents will be required to provide proof of their authorization and we may also require that the relevant consumer directly verify their identity and the authority of the authorized agent.



Under the CCPA, California residents have the following rights (subject to certain limitations and exemptions):

To know/access. You have the right to request that we provide to you the following information about our collection and use of your personal information:

1. The categories of personal information we have collected about you.
2. The categories of sources for the personal information we have collected about you (e.g., use of cookies, third party, etc.).
3. Our business or commercial purpose for collecting, selling or sharing that personal information.
4. The categories of third parties to whom we have disclosed that personal information.
5. The specific pieces of personal information we collected about you (also called a data portability request).

Opt-out of sales and sharing. You have the right to opt-out of our sale and sharing of your personal information. In addition, if we have not disclosed your personal information for a business purpose, we will disclose this fact to you. If we have disclosed your personal information for a business purpose, including direct marketing, we will provide you with a listing that identifies the personal information categories that each category of recipient obtained.

Limit uses and disclosure of sensitive personal information. California residents have the right to limit our use or disclosure of sensitive personal information to those authorized by the CCPA.

Deletion. You have the right to request that we delete any of the personal information collected from you and retained, subject to certain exceptions and your verification. Your request to delete the personal information collected may be denied if it is necessary for us to retain your information under one or more exceptions listed in the CCPA.

Correction. You have the right to correct inaccurate personal information that we maintain about you.

Non-discrimination. You have the right not to be subject to discriminatory treatment for exercising your rights under the CCPA.

WE DO NOT SELL OR SHARE YOUR PERSONAL INFORMATION

We do not sell or share personal information/sensitive personal information as such terms are defined under CCPA, however we do allow third parties to collect certain information about your activity through the use of cookies to the extent you decide to accept such cookies. We may disclose your personal information to our service providers or as instructed by you from time to time for the purpose of providing our services and as detailed above under the section titled "[WHEN DO WE DISCLOSE YOUR INFORMATION?](#)".

The term "sale" is defined as disclosing or making available to a third-party personal information in exchange for monetary or other valuable consideration, and the term "share"



broadly includes disclosing or making available personal information to a third party for purposes of cross-context behavioral advertising.

For more information about our privacy practices, you may contact us as set forth in the Section above titled ["CONTACT US, QUESTIONS, UPDATING YOUR INFORMATION, OPTING OUT"](#).



APPENDIX 4: ADDITIONAL TERMS FOR BRAZILIAN RESIDENTS

The information below is required pursuant to the Brazilian General Law on Data Protection (“**LGPD**”) regarding privacy and data protection. The terms below apply to our Brazilian customers and websites visitors, in addition to the terms in the rest of the Policy.

WHEN DO WE DISCLOSE YOUR PERSONAL INFORMATION?

The table headed “*How and Why We Disclose Your Information*” in the main part of the Policy under the heading “[WHEN DO WE DISCLOSE YOUR INFORMATION?](#)” lists who we may disclose your information to, which include transfers for reasons of legal compliance and necessity in order to provide you with our services.

You should be aware that when you disclose your information, it may be transferred to, and stored at, a destination outside Brazil.

Please note that where data is transferred outside Brazil, such third countries may not offer the same level of protection for personal data as provided in LGPD. Payoneer will take various measures to ensure that your data is treated securely.

Please contact us at DPO@payoneer.com if you require more detailed information about international transfers of your personal information, and the particular safeguards used.

LEGAL BASES FOR PROCESSING YOUR PERSONAL DATA

We process your personal information based on the following legal bases, as recognised by and in compliance with LGPD:

- the processing is necessary to perform our contract with you (i.e. the Terms and Conditions that apply as applicable with respect to our services, for the provision of our services), or to take steps requested by you before entering into said contract;
 - you are obliged to provide us with personal data as it is necessary to enter into and perform our contractual agreements. In the event that you do not wish to provide us with your personal data for the purposes outlined above in the “[HOW AND WHY WE USE YOUR INFORMATION?](#)” section, we will not be able to perform our contractual agreement with you;
- the processing is in Payoneer's or someone else's legitimate interests, and these interests are not overridden by your fundamental rights and freedoms in the protection of your personal data. This may include processing your data for prevention of fraudulent activity, internal research and analytics assessments, for purposes of communication with you, and informing you about new products and services we are offering or to promote new products and services of other parties which we think may be of interest to you, etc.;;
 - before we process your personal data to pursue our legitimate interests for the purposes outlined above in the “[HOW AND WHY WE USE YOUR INFORMATION?](#)” section, we determine if such processing is necessary and we



carefully consider the impact of our processing activities on your fundamental rights and freedoms. On balance, we have determined that such processing is necessary for our legitimate interests and that the processing which we conduct does not adversely impact on these rights and freedoms.

- you have given your consent to the processing of your data;
- the processing is necessary to meet a legal obligation which applies to Payoneer.

Sometimes we process data about you which the law considers sensitive data (see section "[HOW, WHEN AND WHAT WE COLLECT?](#)" for more details), in which case, we use one of the following grounds:

- the processing is necessary for the establishment, exercise or defence of legal claims;
- you have freely given your informed, specific consent to the processing; or
- the processing is necessary for reasons of substantial public interest, based on applicable law.

If you would like more information about the legal grounds used to process your information, or about the legitimate interests referred to above, please contact us.

In cases where we have asked for, and you have given, your consent to our processing of your personal data, you have the right to withdraw such consent at any time. You can do this by contacting our DPO at DPO@payoneer.com.

DO YOU HAVE TO GIVE US YOUR PERSONAL INFORMATION?

In most cases, providing your personal data to us is optional, however, if you do not provide it, you will not be able to use our services. For example, we need details such as your name, address and bank account details so that we can make payments to your account. In other cases, you have a choice over whether we collect your personal data, for example, you can turn off cookies on your browser and we will not place any cookies on your device or computer (although in this case you may not be able to use all parts of our websites) – for additional details regarding cookies and cookie preferences kindly refer to our "[Cookies Policy](#)".

PROFILING AND AUTOMATED DECISION MAKING

We may use automated decision making as part of our process to evaluate eligibility for the use of our services. Such decision-making processes are solely automated and do not require human intervention. We use these tools as a measure of fraud prevention and for the purposes of security and risk assessment relating to the performance of our services, to comply with applicable "Anti Money Laundering" (**AML**) and "Know Your Customer" (**KYC**) rules and to verify your identity when you become a customer, including for example:

- (i) Automated tools incorporated in our process of approval of your registration application: based on the information you provide, the tool may advise if additional information is required for purpose of approval of your application.



- (ii) Automated tools incorporated in our process of approval of certain payment transaction of registered users: such tools may advise if additional information is required for purpose of performance of the payment transaction.
- (iii) Automated tools used to verify your identity to enable us to comply with AML and KYC rules applicable to us as a financial services provider. For example, we carry out this process using selfies (*self-photographs*) and other forms of ID when you register to open an account with us and may also use tools that scan documents for authenticity, classify documents into types, extract required information from the document, approve or decline the sufficiency of documents you submit and determine if additional information or documents are required.

You have certain rights in respect of automated decision making, where the decision taken has significant effects on you, as detailed below in the "YOUR RIGHTS UNDER LGPD" section.

HOW LONG DO WE KEEP YOUR PERSONAL INFORMATION?

Payoneer retains your personal data for the duration of your engagement with us and for a period following termination of your engagement with us, as required or permitted by applicable laws or regulations and/or in accordance with Payoneer's internal policies and procedures for purposes of prevention of fraudulent activity, risk management and security. Payoneer will periodically review the necessity of retention of your personal data.

YOUR RIGHTS UNDER LGPD

You have several rights in relation to your personal data which are described in more detail below. You can exercise your rights at any time.

For requests related to deleting your personal data or receiving a copy of your personal data, you can contact us at any time by using this [online form](#).

For additional queries related to privacy and personal data you can contact our Data Protection Officer at DPO@payoneer.com

Confirming and accessing your data

You can ask us to:

- Confirm whether we are processing your personal data.
- Give you a copy of that personal data.

You do not have to pay a fee for a copy of your personal data unless your request is unfounded, respective or excessive, in which case we will charge a reasonable amount in the circumstances. We will let you know of any charges before completing your request.

Rectifying your personal data

You can ask us to correct any personal data which is incomplete, inaccurate or out-of-date. This is free of charge. If we have disclosed the personal data to anyone else, we will tell them about the correction wherever possible. If we cannot action a request to correct your personal data, we will let you know and explain why this is.



Anonymizing, blocking and erasing your personal data

Subject to the retention provisions above, you may request anonymization, blocking or erasure of unnecessary or excessive personal data, or personal data processed in non-compliance with the provisions of the LGPD. If we have disclosed the personal data to anyone else, we will tell them about the anonymization, blocking or erasure wherever possible. If we cannot action a request to anonymize, block or erase your personal data, we will let you know and explain why this is.

Erasing your personal data processed on the basis of your consent

Subject to the retention provisions above, you can ask us to delete your personal data where it is being processed based on your consent. This right does not arise to the extent that we use another legal basis for processing, such as where processing is necessary for compliance with a legal or regulatory obligation. If we have disclosed the personal data to anyone else, we will tell them about the erasure wherever possible.

Information about disclosure of your personal data

This allows you to obtain information about the entities and third parties to which we have disclosed your personal data. This right is not absolute. We may not be able to comply with this request if the disclosure of personal data is related to an investigation or a processing activity subject to a secrecy obligation.

Information about not giving your consent

You have the right to be informed about the possibility of denying your consent and the consequences of such denial.

As mentioned under the heading "[DO YOU HAVE TO GIVE US YOUR PERSONAL INFORMATION?](#)" above, in most cases, providing your personal data to us is optional, however, if you do not provide it, you will not be able to use our services.

Withdrawing your consent

Where we are processing your personal data based on your consent, you may withdraw it at any time. If we have disclosed the personal data to anyone else, we will tell them about the withdrawal of your consent wherever possible.

Objecting to the processing of your personal data

You have a right to object to the processing of your personal data at any time. This request will be free of charge. It is not an absolute right, but you can object to our processing of your personal data where you believe it is in breach with LGPD provisions. You can require us to stop using your personal data for direct marketing purposes. We will stop as soon as we receive your request. There are no exemptions or reasons for us to refuse.

Data Portability

This allows you to obtain and reuse your personal data for your own purposes across different services, subject to the protection of our commercial or industrial secrets. It applies where the following conditions are met:



- you provided the personal data to us yourself;
- we are processing the personal data either based on your consent or because it is necessary for the performance of a contract; and
- the processing is carried out by automated means.

We will provide your personal data free of charge in a structured, commonly used and machine-readable form.

Revision of automated decision making

You have the right to request the revision of any decisions that we have taken solely based on automated processing of your personal data.

This right is not absolute. We may not be able to comply with this request if the processing of personal data is:

- necessary for us to enter into or perform a contract with you;
- authorised by law (e.g., for fraud prevention) and which also lays down suitable measures to safeguard your right, freedoms and legitimate interests; or
- based on your explicit consent.

Dealing with requests to exercise your rights

We will respond to your request without undue delay at the term provided by LGPD, ANPD's guidelines or specific regulations. We will let you know if we are going to take longer than the required term in dealing with your request. If we have a lot of information about you, we might ask you if you can tell us what exactly you want to receive. This will help us action your request more quickly.

For the purpose of complying with your requests to exercise the rights listed above, we shall perform the necessary internal processes to identify you.

If you are unhappy about how we are processing your data or how we have responded to a request or complaint, you have the right to make a complaint to ANPD.



APPENDIX 5: ADDITIONAL TERMS FOR MAINLAND CHINA RESIDENTS

The information below is required pursuant to the Personal Information Protection Law (“PIPL”) as well as other applicable laws and regulations regarding privacy and data protection in People’s Republic of China, which for the purpose of this Policy, shall exclude Hong Kong, Macao and Taiwan (“China”). The terms below apply to our Chinese customers and websites visitors in Mainland China, in addition to the terms in the rest of the Policy.

LEGAL BASES FOR PROCESSING YOUR PERSONAL DATA

We process your personal information based on the following legal bases, as recognised by and in compliance with PIPL:

- you have given your consent to the processing of your personal information (including the separate consent or written consent as required in PIPL for certain circumstances);
- the processing is necessary for the conclusion or performance of a contract with you;
- the processing is necessary to respond to public health emergencies or protect the life, health or property safety of individuals under emergency circumstances;
- the processing is within a reasonable scope for the purpose of conducting news reporting, public opinion-based supervision, or other activities for the public interest;
- the processing is within a reasonable scope to those data that has been disclosed by you or has been legally disclosed or made public;
- any other circumstance as provided by the law or administrative regulation.

YOUR RIGHTS UNDER THE PIPL

The PIPL gives you the right to access, copy, correct, supplement and delete your personal information, as well as to protect your right to withdraw your consent to the processing of personal information.

You can exercise your rights at any time through the various communication channels available, as listed under the section titled “[CONTACT US, QUESTIONS, UPDATING YOUR INFORMATION, OPTING OUT](#)”.

Please remember that you may need to prove your identity when exercising your rights.

HOW LONG DO WE KEEP YOUR PERSONAL INFORMATION?

Payoneer retains your personal information for the duration of time necessary to achieve the processing purpose and as required by applicable laws or regulations and/or in accordance with Payoneer’s internal policies and procedures for purposes of prevention of fraudulent activity, risk management and security.



To the extent our products or services will be discontinued, we will notify you and delete your personal information or anonymize it within a reasonable period of time.

AUTOMATED DECISION MAKING

We may use automated decision making as part of our process to evaluate eligibility for the use of our services. Such decision-making processes are solely automated and do not require human intervention. We use these tools as a measure of fraud prevention and for the purposes of security and risk assessment relating to the performance of our services, to comply with applicable “Anti Money Laundering” (**AML**) and “Know Your Customer” (**KYC**) rules and to verify your identity when you become a customer, including for example:

- Automated tools incorporated in our process of approval of your registration application: based on the information you provide, the tool may advise if additional information is required for purpose of approval of your application.
- Automated tools incorporated in our process of approval of certain payment transaction of registered users: such tools may advise if additional information is required for purpose of performance of the payment transaction.
- Automated tools used to verify your identity to enable us to comply with AML and KYC rules applicable to us as a financial services provider. For example, we carry out this process using selfies (*self-photographs*) and other forms of ID when you register to open an account with us and may also use tools that scan documents for authenticity, classify documents into types, extract required information from the document, approve or decline the sufficiency of documents you submit and determine if additional information or documents are required.

Where a decision that has a major impact on your rights and interests is made by means of automated decision-making, you have the right to request for explanations and you have the right not to be subject to a decision which is based solely on automated processing.

COLLECTION AND STORAGE OF PERSONAL INFORMATION

You should be aware that your personal information is collected overseas and that such personal information is necessary for Payoneer in order to provide you with our services. Your personal information will be collected and stored at a destination outside China.



APPENDIX 6: ADDITIONAL TERMS FOR HONG KONG RESIDENTS

The information below is required pursuant to Hong Kong law regarding privacy and data protection. The terms below apply to our Hong Kong customers and websites visitors, in addition to the terms in the rest of the Policy.

HOW, WHEN AND WHAT WE COLLECT?

The provision of your personal information to us in accordance with the Policy is voluntary. However, if you do not provide us with the information requested, we may not be able to deliver the services to you, or the delivery of the services may be affected.

HOW AND WHY WE USE YOUR INFORMATION?

The section "[HOW AND WHY WE USE YOUR INFORMATION?](#)" in the main part of the Policy lists uses of personal information that include direct marketing. We comply with the direct marketing requirements of the Hong Kong Personal Data (Privacy) Ordinance (Cap. 486 of the Laws of Hong Kong) ("PDPO").

If we intend to use your personal data (i.e., your name and contact information) for marketing purposes, we must first obtain your express consent. If we intend to disclose such information to any third party for marketing purposes, we must first obtain your written consent.

You can exercise your right to prevent such use or transfer of personal data for direct marketing by checking certain boxes when we ask you whether you object to our using or transferring your personal data in this way. If you consent to such use or transfer, you may also exercise the right to withdraw your consent at any time by contacting us through the various communication channels available, as listed under the section titled "[CONTACT US, QUESTIONS, UPDATING YOUR INFORMATION, OPTING OUT](#)" in the main part of the Policy, or by unsubscribing from any marketing emails sent to you by Payoneer using a link provided in the email.

The third item in the table headed "***How and Why We Disclose Your Information***" in the main part of the Policy under the heading "[WHEN DO WE DISCLOSE YOUR INFORMATION?](#)" lists whom we may disclose your personal data to for marketing purposes (with your consent). To elaborate, we may disclose your personal data to the following third parties for marketing purposes:

1. With our affiliates;
2. With our service providers who provide us with marketing related services; and
3. With other non-affiliated third parties (including financial institutions and platforms) for joint marketing purposes.

When opted in, we and such third parties may send you marketing information with respect to Payoneer products and services, including such which are in provided in collaboration with said third parties.



YOUR RIGHTS UNDER THE PDPO

The PDPO gives you the right to access and to be supplied with a copy of personal data held about you and the right to rectify that personal data if it is inaccurate.

You can exercise your rights at any time through the various communication channels available, as listed under the section titled "[CONTACT US, QUESTIONS, UPDATING YOUR INFORMATION, OPTING OUT](#)".



APPENDIX 7: ADDITIONAL TERMS FOR JAPANESE RESIDENTS

When using our payment services on Amazon, we will jointly use the categories of personal data listed under (i) below with Amazon for the purposes listed under (ii) below in accordance with Article 27.5.3 of Act on Protection of Personal Information. Each of us ([Please see <https://www.payoneer.com/ja/about/> for our address and our representative director's name](https://www.payoneer.com/ja/about/)) and Amazon will be responsible for the management of the jointly used personal Data held thereby.

(i) Categories of Personal Data Jointly Used

We may disclose all or part of the details collected during the account sign-up process and when you use your account as below.

- “Know Your Client” data and other which includes identity data (e.g., name, nationality), contact information (e.g., address) and details regarding your Payoneer accounts and bank accounts.
- If your Amazon account is deactivated or terminated by Amazon due to abuse, fraud or illegal activity, we may disclose additional information, including limited transaction related information.

(ii) Purposes of the Joint Use

The data will be used for the purposes of Amazon’s Payment Service Provider Program, designed to enhance its ability to detect, prevent and take action against bad actors so Amazon and participating PSPs can continue to protect customers and sellers from fraud and abuse.



APPENDIX 8: ADDITIONAL TERMS FOR SOUTH AFRICAN RESIDENTS

The information below is required pursuant to laws in South Africa regarding privacy and data protection. The terms below apply to our South African customers and websites visitors, in addition to the terms in the rest of the Policy.

For the purposes of the Protection of Personal Information Act, 2013 (“**POPIA**”), the data controller / responsible party is Payoneer Inc. If you have any questions about this Policy, please contact DPO@payoneer.com.

If you are unhappy about how we are processing your personal information or how we have responded to a request or complaint, you have the right to make a complaint to the Information Regulator in South Africa, the details of which are as follows:

The Information Regulator (South Africa)

JD House

27 Stiemens Street

Braamfontein

Johannesburg

2001

Email: inforeg@justice.gov.za / complaints.IR@justice.gov.za

DEFINITION OF PERSONAL INFORMATION IN TERMS OF POPIA

In South Africa in terms of POPIA *Personal Information* means information relating to an identifiable, living, natural person and where applicable, an identifiable, existing juristic person. Reference to personal data or personal information in this policy with respect to South African Customers shall mean personal information as defined in POPIA.

LEGAL BASES FOR PROCESSING YOUR PERSONAL INFORMATION

We process your personal information based on the following legal bases, as recognised by and in compliance with POPIA:

- the processing is necessary to perform our contract with you (i.e. the Terms and Conditions that apply as applicable with respect to our services, for the provision of our services), or to take steps requested by you before entering into said contract;



- you are obliged to provide us with personal information as it is necessary to enter into and perform our contractual agreements. In the event that you do not wish to provide us with your personal information for the purposes outlined above in the "[HOW AND WHY WE USE YOUR INFORMATION?](#)" section, we will not be able to perform our contractual agreement with you;
- the processing is in Payoneer's or someone else's legitimate interests. This may include processing your personal information for identification or prevention of suspicious or high risk transactions or fraudulent activity, internal research and analytics assessments, for purposes of communication with you, and informing you about new products and services we are offering or to promote new products and services of other parties which we think may be of interest to you, etc.;
- you have given your consent to the processing of your personal information;
- the processing is necessary to meet a legal obligation which applies to Payoneer.

Sometimes we process personal information about you which POPIA defines as special personal information, in which case, we use one of the following grounds:

- the processing is necessary for the establishment, exercise or defence of a right or obligation in law; or
- you have freely given your informed, specific consent to the processing.

If you would like more information about the legal grounds used to process your personal information, or about the legitimate interests referred to above, please contact us.

In cases where we have asked for, and you have given, your consent to our processing of your personal information, you have the right to withdraw such consent at any time. You can do this by Emailing us or by contacting Payoneer Customer Care as detailed under paragraph "[CONTACT US, QUESTIONS, UPDATING YOUR INFORMATION, OPTING OUT](#)" in the Policy.

DO YOU HAVE TO GIVE US YOUR PERSONAL INFORMATION?

In most cases, providing your personal information to us is optional, however, if you do not provide it, you will not be able to use our services. For example, we need details such as your name, address and bank account details so that we can make payments to you and receive payments from you. In other cases, you have a choice over whether we collect your personal information, for example, you can turn off cookies on your browser and we will not place any cookies on your device or computer (although in this case you may not be able to use all parts of our websites).

YOUR RIGHTS UNDER POPIA

In terms of POPIA you have the following rights in relation to your personal information:



- to request access to, and information regarding the nature of personal information held and to whom it has been disclosed. Such request for access may be refused on the basis of the grounds of refusal in the Promotion of Access to Information Act, 2000;
- to request the restriction of processing of personal information in the circumstances contemplated in POPIA;
- not to be subjected to a decision which is based solely on the automated processing of personal information intended to provide a profile of such person, save for in the circumstances permitted by POPIA;
- to request to rectify or correct personal information that is inaccurate, irrelevant, excessive, out of date, incomplete, misleading or obtained unlawfully;
- to request deletion of personal information that is inaccurate, irrelevant, excessive, out of date, incomplete, misleading or obtained unlawfully or where we are no longer authorized to retain it;
- to object to processing of personal information where the processing is on the basis that (a) it protects your legitimate interests; (b) it is necessary for pursuing our legitimate interests or that of a third party to whom it is disclosed; or (c) it is for the purposes of direct marketing other than by unsolicited electronic communications;
- to lodge a complaint with the Information Regulator; and
- to institute civil proceedings regarding the alleged interference with the protection of your personal information.

You can exercise your rights at any time.

For requests related to deleting your personal data or receiving a copy of your personal data, you can contact us at any time by using this [online form](#).

For additional queries related to privacy and personal data you can contact our Data Protection Officer at DPO@payoneer.com.



APPENDIX 9: ADDITIONAL TERMS FOR SINGAPORE RESIDENTS

The information below is required pursuant to laws in Singapore regarding privacy and data protection. The terms below apply to customers of Payoneer Singapore Private Limited and websites visitors in Singapore, in addition to the terms in the rest of the Policy.

For the purposes of the Personal Data Protection Act 2012, the data controller / responsible party is Payoneer Singapore Private Limited. If you have any questions about this Policy, please contact DPO@payoneer.com.

HOW, WHEN AND WHAT WE COLLECT?

The provision of your personal information to us in accordance with the Policy is voluntary. However, if you do not provide us with the information requested, we may not be able to deliver the services to you, or the delivery of the services may be affected.

We collect, use and/or disclose your personal information with your consent, where required to do so under applicable law.

Where you have provided us with the personal information of third parties (e.g., your colleagues), you acknowledge that you have the right and are duly authorized to provide us with the personal information of these third parties.

YOUR RIGHTS UNDER THE PDPA

The PDPA gives you the right to access (including the right to request information on how your personal information has been used and disclosed by us in the 12 months prior to your request) and correct your personal information. You also have the right to withdraw your consent to the processing of your personal information. Depending on the nature of your withdrawal, we may not be able to continue providing our services to you, or the delivery of our services to you may be affected.

You can exercise your rights at any time through the various communication channels available, as listed under the section titled "[CONTACT US, QUESTIONS, UPDATING YOUR INFORMATION, OPTING OUT](#)".

Please remember that you may need to prove your identity when exercising your rights. Where we are permitted to do so under applicable law, we may charge you a reasonable fee for processing your request.



APPENDIX 10: ADDITIONAL TERMS FOR REPUBLIC OF KOREA RESIDENTS

The terms below apply to our Korean customers and Website visitors in the Republic of Korea, in addition to the terms in the rest of the Policy. Please note that you have the right to refuse to provide consent to the collection, use and third-party provision of personal information as stated in the Policy and this Appendix, however, in such case, you may not be able to utilize the services.

HOW DO WE DESTROY YOUR PERSONAL INFORMATION?

We will destroy personal information without delay when either the purpose of processing has been achieved or the period of processing and retention has expired:

- Personal information stored in the form of an electronic file shall be permanently deleted using a technical method that renders the record irrecoverable.
- Other records, printed materials, written documents or recording media shall be destroyed by shredding or incinerating them.

HOW DO WE PROTECT YOUR PERSONAL INFORMATION?

To ensure the safety of information, we apply highest industry standards of administrative, technical and physical measures to protect your personal information in accordance with GDPR. For more information, please contact DPO@payoneer.com.

DISCLOSURE OF YOUR PERSONAL INFORMATION

The third parties we share your personal information with are dependant on your specific use of our services, and therefore, we do not maintain an online list of such third parties. If you would like additional information about third parties we have shared your personal data with, please contact DPO@payoneer.com.

RIGHTS OF DATA SUBJECTS AND METHODS TO EXERCISE RIGHTS ON PERSONAL INFORMATION

You may exercise rights related to the protection of personal information by requesting access to your personal information or the correction, deletion or suspension of processing of your personal information, etc. in writing or via email, phone, etc. pursuant to applicable laws. You may also exercise these rights through your legal guardian or someone who has been authorized by you to exercise such rights. However, in this case, you must submit a power of attorney to us in accordance with applicable laws. Upon your request, we will take necessary measures in accordance with applicable laws. You can also withdraw your consent or demand a suspension of the personal information processing at any time.



ADDITIONAL USE AND PROVISION OF PERSONAL INFORMATION

In accordance with the PIPA, we may use or provide personal information within the scope of reasonably related to the initial purpose of the collection, in consideration of whether disadvantages have been caused to data subjects and whether necessary measures have been taken to secure such as encryption, etc. We will determine with due care whether to use or provide personal information in consideration of general circumstances including relevant laws and regulations such as the PIPA, purpose of use or provision of personal information, how personal information will be used or provided, items of personal information to be used or provided, matters to which data subjects provided consent or which were notified/disclosed to data subjects, impact on data subjects upon the use or provision, and measures taken to protect subject information. Specific considerations are as follows:

- Whether the additional use/provision is related to the initial purpose of collection;
- Whether the additional use/provision is foreseeable in light of the circumstances under which personal information was collected and practices regarding processing;
- Whether the additional use/provision unfairly infringe on the interests of the data subject; and
- Whether necessary security measures to protect such personal information were taken.



APPENDIX 11: ADDITIONAL INFORMATION FOR RESIDENTS OF THE UNITED KINGDOM

The information below is required pursuant to UK law regarding privacy and data protection and applies to our UK customers of Payoneer Payment Services (UK) Limited and websites visitors), in addition to the information in the rest of the Policy.

For the purposes of the UK data protection laws, the data controller is Payoneer Payment Services (UK) Limited of 37 Broadhurst Gardens, London, England, NW6 3QT, a company established in the United Kingdom and regulated for data protection purposes by the Information Commissioner's Office (UK ICO). If you have any questions about this Policy, please contact our Data Protection Officer (DPO) at DPO@payoneer.com.

If you are unhappy about how we are processing your personal information or how we have responded to a request or complaint, you have the right to make a complaint to the UK ICO. You can find more details about how to contact the UK ICO on their [website](#).

WHEN DO WE DISCLOSE YOUR PERSONAL INFORMATION?

The table headed "*How and Why We Disclose Your Information*" in the main part of the Policy under the heading "[WHEN DO WE DISCLOSE YOUR INFORMATION?](#)" lists who we may disclose your information to, which includes transfers for reasons of legal compliance and necessity in order to provide you with our services.

You should be aware that when you disclose your information, it will be transferred to, and stored in, countries outside the UK, as applicable, including the USA and Israel.

Please note that where data is transferred outside of the UK, these countries may not offer the same level of protection for personal information as is available in the UK. Payoneer will take various measures to ensure that your data is treated securely, which may include, but not be limited to:

- assessing the security measures taken at any place your personal information is transferred to;
- having suitable contract terms in place that oblige a service provider / data processor to only process in accordance with our instructions;
- having monitoring, reporting and resolution procedures in place with regard to ongoing security; and
- only transferring your personal information to countries that have been assessed by the UK as offering an adequate level of data protection or implementing appropriate safeguards as necessary, which may include contractual clauses adopted by the UK ICO such as the [UK International Data Transfer Agreement](#).

Please contact us at DPO@payoneer.com if you require more detailed information about international transfers of your personal information, and the safeguards applied.



LEGAL BASES FOR PROCESSING YOUR PERSONAL INFORMATION

We process your personal information based on the following legal bases, as recognised by and in compliance with the applicable data protection laws:

- the processing is necessary to perform our contract with you (i.e., the Terms and Conditions that apply with respect to our services, for the provision of our services), or to take steps requested by you before entering into said contract;
 - you are obliged to provide us with personal information as it is necessary to enter into and perform our contractual agreements. In the event that you do not wish to provide us with your personal information for the purposes outlined above in the "[HOW AND WHY WE USE YOUR INFORMATION?](#)" section, we will not be able to perform our contractual agreement with you;
- the processing is in Payoneer's or someone else's legitimate interests, and these interests are not overridden by your interests or rights in the protection of your personal information. This may include processing your data for identification or prevention of suspicious or high risk transactions or fraudulent activity, internal research and analytics assessments, for purposes of communication with you, and informing you about new products and services we are offering or to promote new products and services of other parties which we think may be of interest to you, etc.;;
 - before we process your personal information to pursue our legitimate interests for the purposes outlined above in the "[HOW AND WHY WE USE YOUR INFORMATION?](#)" section, we determine if such processing is necessary and we carefully consider the impact of our processing activities on your fundamental rights and freedoms. On balance, we have determined that such processing is necessary for our legitimate interests and that the processing which we conduct does not adversely impact on these rights and freedoms.
- you have given your consent to the processing of your data;
- the processing is necessary to meet a legal obligation which applies to Payoneer.

Sometimes we process data about you which the law considers as falling within special categories (see section "[HOW, WHEN AND WHAT WE COLLECT?](#)" for more details), in which case, we use one of the following grounds:

- the processing is necessary for the establishment, exercise or defence of legal claims;
- you have freely given your informed, specific consent to the processing; or
- the processing is necessary for reasons of substantial public interest, based on applicable law.

If you would like more information about the legal grounds used to process your information, or about the legitimate interests referred to above, please contact us.



In cases where we have asked for, and you have given, your consent to our processing of your personal information, you have the right to withdraw such consent at any time. You can do this by contacting our DPO at DPO@payoneer.com.

DO YOU HAVE TO GIVE US YOUR PERSONAL INFORMATION?

In most cases, providing your personal information to us is optional, however, if you do not provide it, you will not be able to use our services. For example, we need details such as your name, address and bank account details so that we can make payments to you and receive payments from you. In other cases, you have a choice over whether we collect your personal information, for example, you can turn off cookies on your browser and we will not place any cookies on your device or computer (although in this case you may not be able to use all parts of our websites).

PROFILING AND AUTOMATED DECISION MAKING

We may use automated decision making as part of our process to evaluate eligibility for the use of our services. Such decision-making processes are solely automated and do not require human intervention. We use these tools as a measure of fraud prevention and for the purposes of security and risk assessment relating to the performance of our services, to comply with applicable "Anti Money Laundering" (**AML**) and "Know Your Customer" (**KYC**) rules and to verify your identity when you become a customer, including for example:

- (iv) Automated tools incorporated in our process of approval of your registration application: based on the information you provide, the tool may advise if additional information is required for the approval of your application.
- (v) Automated tools incorporated in our process of approval of certain payment transaction of registered users: such tools may advise if additional information is required for the performance of the payment transaction.
- (vi) Automated tools used to verify your identity to enable us to comply with AML and KYC rules applicable to us as a financial services provider. For example, we carry out this process using selfies (*self-photographs*) and other forms of ID when you register to open an account with us and may also use tools that scan documents for authenticity, classify documents into types, extract required information from the document, approve or decline the sufficiency of documents you submit and determine if additional information or documents are required.

You have certain rights in respect of automated decision making, where the decision taken has significant effects on you, as detailed below in the "[YOUR RIGHTS UNDER UK DATA PROTECTION LAWS](#)" section.

HOW LONG DO WE KEEP YOUR PERSONAL INFORMATION?



Payoneer retains your personal information for the duration of your engagement with us and for a period following termination of your engagement with us, as required by applicable laws or regulations and/or in accordance with Payoneer's internal policies and procedures for purposes of prevention of fraudulent activity, risk management and security. Payoneer will periodically review the necessity of retention of your personal information.

YOUR RIGHTS UNDER UK DATA PROTECTION LAWS

You have several rights in relation to your personal information which are described in more detail below. You can exercise your rights at any time.

For requests related to deleting your personal information or receiving a copy of your personal information, you can contact us at any time by using this [online form](#).

For additional queries related to privacy and personal information you can contact our Data Protection Officer at DPO@payoneer.com.

Accessing your data

You can ask us to:

- Confirm whether we are processing your personal information.
- Give you a copy of that personal information.
- Provide you with other information about your personal information such as what data we have, what we use it for, who we disclose it to, whether we transfer it outside of the UK and how we protect it, how long we keep it for, what rights you have, how you can make a complaint, where we got your data from and whether we carry out any automated decision making or profiling. We aim to give you all this information in this Policy, although if anything is unclear, please contact our Data Protection Officer at DPO@payoneer.com.

You do not have to pay a fee for a copy of your personal information unless your request is manifestly unfounded, excessive or if you request further copies, in which case we may charge a reasonable amount in the circumstances. We will let you know of any charges before completing your request.

Correcting your personal information

You can ask us to correct any personal information which is inaccurate or incomplete. This is free of charge.

If we have disclosed the personal information to anyone else, we will tell them about the correction wherever possible.

If we cannot action a request to correct your personal information, we will let you know and explain why this is.

Erasing your personal information



This right is sometimes referred to as "the right to be forgotten". This is not an absolute right but you have the right to have your personal information erased, free of charge, in certain circumstances.

You can ask for your personal information to be erased where:

- it is no longer necessary for the purpose for which it was originally collected or processed;
- we are processing your personal information based on your consent, and you withdraw that consent;
- you object to the processing and we do not have an overriding legitimate interest for continuing;
- your personal information has been unlawfully processed;
- your personal information must be erased to comply with a legal obligation;
- the personal information was processed to offer information society services to a child.

There are some exceptions to this right. If one of these applies, we do not have to delete the personal information.

If we have disclosed your personal information to third parties, we will tell them about the erasure of your personal information unless this is impossible or would involve disproportionate effort.

Please note, in connection with such requests, that personal information may be either deleted or retained in an aggregated manner without being linked to any identifiers or personal information, depending on technical commercial capability.

Restricting the processing of your personal information

You can ask us to restrict the processing of your personal information in some circumstances, free of charge. This is not an absolute right. If processing is restricted we can store the personal information and retain enough information to make sure the restriction is respected unless you consent or the processing is necessary in relation to a legal claim or to protect the rights of another person or for reasons of important public interest, but we cannot further process your personal information.

You can restrict the processing of your personal information in the following cases:

- if you contest the accuracy of your personal information, we will restrict processing until we have made sure the personal information is accurate;
- if you object to our processing pending the verification of whether or not our legitimate interests override your interests, rights and freedoms or in connection with legal proceedings;



- if the processing is unlawful but you do not want us to erase your personal information;
- if we no longer need the personal information but you require the data to establish, exercise or defend a legal claim.

If we have disclosed the personal information to a third party, we will inform them about the restriction unless it is impossible or would require a disproportionate effort. We will tell you if we decide to lift a restriction on processing your personal information.

Objecting to the processing of your personal information

You have a right to object to the processing of your personal information at any time. This request will be free of charge. It is not an absolute right, but you can object to our processing of your personal information where it is:

- based on the legitimate interest ground; or
- for the purposes of scientific/historical research and statistics.

We will stop processing your personal information unless we have compelling legitimate grounds for the processing which override your interests and rights, or unless we are processing the personal information for the establishment, exercise or defence of legal claims.

You can require us to stop using your personal information for direct marketing purposes. We will stop as soon as we receive your request. There are no exemptions or reasons for us to refuse.

Data Portability

This allows you to obtain and reuse your personal information for your own purposes across different services. It applies where the following conditions are met:

- you provided the personal information to us yourself;
- we are processing the personal information either based on your consent or because it is necessary for the performance of a contract; and
- the processing is carried out by automated means.

We will provide your personal information free of charge in a structured, commonly used and machine-readable form.

Automated decision making and profiling

You have the right not to be subject to a decision which is based solely on automated processing, and which produces a legal (or similarly significant) effect on you. In certain circumstances where automated decision making is used, you will be provided with an opt-out option by way of an alternative means of processing.



We will tell you about any automated decision making that affects you. You have the right to:

- request human intervention;
- express your point of view; and
- challenge the decision.

These rights are not absolute. We may not be able to comply with your request to obtain human intervention, obtain your point of view or to contest a decision, if the processing of personal information is:

- necessary for us to enter into or perform a contract with you;
- authorised by law (e.g., for fraud prevention) and which also lays down suitable measures to safeguard your right, freedoms and legitimate interests; or
- based on your explicit consent.

Dealing with requests to exercise your rights

We will respond to your request without undue delay at the latest within one (1) month of receiving your request unless it is particularly complicated or you have made several requests, in which case we may extend this by two (2) months. We will let you know if we are going to take longer than one (1) month in dealing with your request. If we have a lot of information about you we might ask you if you can tell us what exactly you want to receive. This will help us action your request more quickly.

For the purpose of complying with your requests to exercise the rights listed above, we shall perform the necessary internal processes to identify you.