IDT Financial Services Limited

Privacy Notice

Effective and Updated as of May 25, 2018

I. Who we are

IDT Financial Services Limited ("IDT") gathers and processes your personal data in accordance with this notice and in compliance with the relevant data protection regulations and laws. This notice provides you with the necessary information regarding your rights and our obligations, and explains how, why and when we process your data. We are committed to protecting the privacy of your data.

IDT acts as a data controller when processing your personal data, which means that we determine the purposes and means of the processing of your personal data collected by us. IDT is a company registered in Gibraltar under company registration number 95716. Our contact information is:

IDT Financial Services Limited
1 Montarik House
3 Bedlam Court
Gibraltar
Email: privacy@idtfinance.com
IDT's Data Protection Officer: Giovanni Santini
IDT's Representative's Email: privacy@idtfinance.com

II. Who this notice applies to

This notice applies to the following people:

- users and holders of cards issued by IDT (the "Cards");
- users and visitors within the EU of/to the website: www.idtfinance.com (the "Website").

When we use the term "Services" in this notice it refers to the Cards, the Website, and services provided by IDT in connection with the Cards, their operation and administration.

The Cards are marketed, distributed, and supported by third parties ("Program Managers") under various brands. You should also refer to the respective privacy policies and notices published by these Program Managers with respect to the treatment any personal information provided in relation to the Services, as these Program Managers may use your personal information in different ways to IDT, and for different purposes. Our corporate affiliate IDT Retail Europe Limited markets Cards under the "Prime" brand. If you are a user or holder of this Card then you should also refer to the privacy policy on the website

You should also read the terms and conditions for each Card that you use. We may update this notice from time to time and you should review it periodically for changes. Any updated notice will be posted on the Website.

III. Data we collect and how we collect it

IDT receives and collects both personal and non-identifying data upon your registration, or enrollment for a Card, issuance to you of Card, your use of Card, our provision of services necessary in the operation, or administration of a Card, and when you communicate with us. We may also collect personal data and non-identifying data about you from Program Managers or their subcontractors. Personal data means information either on its own or in conjunction with other data that enables a specific person to be identified, but does not include "de-identified," "anonymous," or "aggregate" information, which is not otherwise associated with a specific person. Non-identifying data means data that by itself cannot be used to identify a specific person. We do not receive or collect any personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and we do not process genetic data or biometric data, data concerning health or data concerning a natural person's sex life or sexual orientation. We will never collect any unnecessary personal data from you.

The personal data that we collect from you or about you is:

A. Data you provide. Depending on the particular Service you use, you may provide the following data directly to us:

- name
- address, including country of residence
- email address
- mobile phone number
- payment information, including credit or debit card details
- birthdate

- government issued ID
- driving license
- utility bills
- other personal information you provide to us for customer support purposes

B. Data we collect from you. Depending on the particular Service you use, we may automatically collect the following data from you or your device:

- security code, password and login credentials

- type, application software, mobile network, device identifiers and numbers, and Internet connection speed
- IP address

C. Data provided by third parties. Depending on the particular Service you use, we may obtain the following information on you via third party tools and systems that allow us to perform governmental sanctions checks.

III. How we use your personal data

A. General. IDT takes your privacy very seriously and will never disclose, share or sell your personal data without your consent, except as set forth in this notice or required to do so by law. We do not process your data in any way other than as specified in this notice and we retain your data only for as long as is necessary.

B. Specific use of your personal data. More specifically, the purposes, legal basis and reasons for processing your personal data are detailed below:

How we use your data	Our legal basis	Our reasons for using your data this way
● To communicate with you about our terms, policies, and other important information regarding our Services ● To manage our Services, including to help us operate, provide, evaluate, improve, monitor, customize, bill and support our Services ● To verify your account and activity and investigate any suspicious activity or violations of our terms ● To perform due diligence and credit and fraud prevention checks ● To maintain accurate record keeping and data back up ● To detect, investigate, report, and seek to prevent fraud, abuse or illegal use of our Services and crime ● To manage risk for us and our customers ● To comply with laws and regulations that apply to us ● To obtain legal advice and/or defend IDT ● To respond to customer service issues and complaints and seek to resolve them	**Legal and Vital Interests of Data Subjects**	● Fulfilling our legal duties to our customers ● Complying with regulations and legal requirements that apply to us ● Providing and supporting our Services ● General, operational and administrative purposes, including customer service and audit functions ● Risk management and compliance, including, compliance with financial services and anti-money laundering regulations ● Legal advice and defense
● To perform our obligations under our Cardholder terms and conditions, including providing services in connection with the operation of the Cards and the transactions performed using the Cards ● To manage our relationship with you, including maintaining your account and authenticating you ● To communicate with you about our terms, policies, and other important information regarding our Services ● To manage our Services, including to help us operate, provide, evaluate, improve, monitor,	**Contract**	● Exercising our rights set out in Cardholder terms and conditions or contracts with our customers and vendors, whether formal or informal ● Fulfilling our contractual duties to our customers ● Complying with contractual requirements ● Providing and supporting our Services ● General, operational and administrative purposes, including customer service

customize, bill and support our Services ● To verify your account and activity and investigate any suspicious activity or violations of our terms ● To perform due diligence and credit and fraud prevention checks ● To collect a debt ● To troubleshoot Service issues ● To manage how we work with other companies that provide services to us and our customers ● To respond to customer service issues and complaints and seek to resolve them		
● To communicate with you about our terms, policies, and other important information regarding our Services ● To manage our relationship with you, including maintaining your Card and authenticating you ● To manage our Services, including to help us operate, provide, evaluate, improve, monitor, customize, bill and support our Services ● To verify your account and activity and investigate any suspicious activity or violations of our terms ● To perform due diligence and credit and fraud prevention checks ● To maintain accurate record keeping and data back up ● To manage risk for us and our customers ● To troubleshoot Service issues ● To respond to customer service issues and complaints and seek to resolve them[1] ● To detect, investigate, report, and seek to prevent fraud, abuse or illegal use of our Services and crime ● To ensure the security of our network and information	**Legitimate Interest**	● Ensuring we provide the level of service that our customers expect, in line with any Cardholder terms and conditions ● Fulfilling our contractual duties to our customers ● Providing, improving, understanding, customizing and supporting our Services ● General, operational and administrative purposes, including customer service ● Improving the quality and value of our Services ● Understanding how our Services are used

C. Automated decision making. At times we will use systems to make automated decisions based on your personal data. This enables us to make quick and fair decisions, based on what we know. These automated decisions can affect your registration for our Services, transactions you have performed or attempt to perform using our Cards, or features available to you. We use your data to make automated decisions mainly for (a) ecommerce risk management in order to spot any activity that could potentially be fraudulent or criminal, (b) in fulfillment of anti-money laundering and other compliance requirements, and (b) to understand how you use our Services. If we think there is a risk of fraud or criminal activity, or

our compliance alerts are triggered, we may take action such as denying a transaction or refusing registration for a Card.

IV. How we share your personal data

We will never disclose, share or sell your personal data without your consent, except as set forth in this notice or required to do so by law. We share all the information we collect and receive with our affiliates, both in and outside the EU, and to select third parties, to help us operate, provide, improve, understand, customize, support, and market our Services, and for general, operational and administrative purposes, including operating and administering the Cards and any transactions performed on or using the Cards, authenticating you, or contacting you. All third party data processors acting on our behalf only process your data in accordance with instructions from us and are required to comply fully with this notice, the relevant data protection laws and any other appropriate confidentiality and security measures. IDT does not sell your data to third parties without your consent. IDT does not sell, rent or lease its customer lists to third parties. Finally, you share your information as you use and communicate through our Services.

A. Data shared within the IDT family of companies. IDT shares certain Cardholder data within the IDT Telecom, Inc. family of companies ("IDT Family of Companies") for security, operational and general administration purposes. This includes sharing information with entities (and the servers operated by those entities) in the IDT Family of Companies that are based in the USA. In applying for a Card and associated accounts and services from IDT you explicitly consent to this. Please note that the legal regimes of some territories outside of the European Economic Area ("EEA") do not always offer the same standard of data protection as those inside the EEA, although we will ensure that your personal information is only ever treated in accordance with this policy, and if you are a cardholder, our terms and conditions. Any transfer of personal information is governed by a data transfer agreement between IDT and the IDT Family of Companies, incorporating the EU standard model contract clauses for data transfer outside the EU.

B. Data shared with third parties. We share data with the following categories of third parties for the reasons stated below. We require that all these processors protect your data and limit their use of the data solely for the purposes for which it was provided. Moreover, we require that these processors comply fully with this notice, the relevant data protection laws and any other appropriate confidentiality and security measures. Finally, if you use Cards offered jointly by IDT and one of our Program Managers, your personal data may be received by both IDT and the Program Manager that is marketing the Card. For these jointly offered Services, you should also review the Program Manager's privacy notice, which may include practices that are different from the practices described here.

1. Card Processors. We work entities known as payment card processors that use your personal information to facilitate the settlement of transactions performed on or using the Cards. We share data with these people solely to the extent reasonably necessary for them to perform work on our behalf and under a strict code of confidentiality.

2. Card Manufacturers. The Cards issued by IDT are manufactured by certain payment card manufacturers. Card manufacturers require certain personal information so that they can populate a Card with the Cardholder's name, and in certain cases, the Cardholder's address for mailing purposes.

C. Special Circumstances. We may share your data with various government, administrative and law enforcement agencies, regulators or other third parties in the following special circumstances:

- to comply with valid legal process including subpoenas, court orders, warrants, and as otherwise permitted or required by law;
- to assist law enforcement in cases involving national security, defence, public security, danger, death or serious physical injury to any person or in other emergencies;
- to fulfill our reporting obligations in accordance with anti-money laundering laws;
- to assist law enforcement in the prevention, investigation, detection or prosecution of criminal offences, including the safeguarding against and the prevention of threats to public security;
- to protect our rights or property, or the safety of our customers or employees;
- to protect against fraudulent, malicious, abusive, unauthorized or unlawful use of our Services and to protect our network, Services, devices and users from such use;
- to advance or defend against complaints or legal claims in court, administrative proceedings and elsewhere;
- to prospective purchasers of all or part of our business or assets; and
- with your consent.

V. Your rights

A. General. IDT takes measures to protect your data and keep it private, but your privacy is also protected by law. Under the General Data Protection Regulation ("GDPR") you have certain access rights regarding your personal data and we are only allowed to use your personal data if we have a valid reason to do so. In addition, we comply with the data protection principles of the GDPR, meaning that your personal data is:

- processed lawfully, fairly and in a transparent manner;
- collected for specified, explicit and legitimate purposes as set forth in this notice and not further processed in a manner that is incompatible with those purposes;
- adequate, relevant and not excessive;
- accurate and complete;
- not kept longer than necessary for the purposes for which the personal data are processed;
- processed in accordance with your rights;
- kept secure; and
- not transferred to countries without adequate protection.

B. Right of access. You have the right to access any personal data that IDT processes about you and to request information about:

- what personal data we process about you;
- the purposes of the processing;
- the categories of personal data concerned;

- the recipients to whom the personal data has/will be disclosed, including recipients in any third country (in which case we will inform you of the appropriate safeguards relating to the transfer);
- how long we intend to store your personal data;
- the existence of other rights you have, including your right to request rectification of any inaccurate personal data held by us, your right to restrict the processing of your personal data or to object to such processing, and the right to data portability;
- your right to lodge a complaint with a supervisory authority;
- the source of any personal data about if that we did not collect directly from you; and
- the existence of automated decision-making, including profiling.

Notwithstanding the above, in certain cases we will not grant access to certain reports that may contain your personal information, where to do so would be in conflict with applicable financial services and anti-money laundering laws and regulations.

C. Right of rectification. You have the right to request rectification of any inaccurate personal data held by us. Where you notify us of inaccurate data about you, and we agree that the data is incorrect, we will amend the details promptly as directed by you and make a note on our system of the change and reasons. We will rectify any errors and inform you in writing of the correction and where applicable provide the details of any third party to whom the data has been disclosed. If for any reason we are unable to act in response to a request for rectification and/or data completion or need more time, we will provide a written explanation to you and inform you of your right to complain to the supervisory authority.

D. Right of erasure (right to be forgotten). You have the right to request erasure of your personal data in certain circumstances, including where the including the data are no longer necessary to the purposes for which it was collected, you withdraw your consent (and there is no other legal basis for processing) or you object to the processing (and we have no overriding legitimated grounds for the processing). Even if you request erasure of your data, we may continue to hold and process such data under certain circumstances, including for compliance with legal obligations.

Notwithstanding the above, in certain cases we will be prohibited from erasing personal information in certain circumstances, where to do so would be in conflict with applicable financial services and anti-money laundering laws and regulations.

E. Right to restrict processing. You have the right to restrict processing of your personal data under certain circumstances (such as the accuracy of the data is contested) and subject to certain exceptions (such as processing for legal claims).

Notwithstanding the above, in certain cases we will not be required to restrict processing where to do so would be in conflict with applicable financial services and anti-money laundering laws and regulations.

F. Right to data portability. You have the right to data portability, meaning the right to receive the personal data concerning you which you have provided us in a commonly used, machine-readable format and to have that data transmitted to another controller (where feasible), if our processing is based on your consent or a contract and the processing is carried out by automated means.

G. Right to object to processing. You have the right to object to any processing of your personal data which is based on our legitimate interests, including profiling, and we shall no longer process such data unless we demonstrate compelling legitimate grounds to do so.

H. Right not to be subject to automated decision. You have the right not to be subject to a decision based solely on automated processing, including profiling, which significantly affects you, subject to certain exceptions including if the decision is necessary for us to perform our contract with you, is authorised by EU or Member State law, is required under applicable financial services or anti-money laundering laws and regulations, or is based on your consent.

I. How to make a request. To make a request for access to your personal data or to exercise any of your other rights, you can email us at privacy@idtfinance.com attaching a completed copy of Appendix 1 to this notice. You can also submit your request using the form in Appendix 1 to this notice and sending that form to us at:

IDT Financial Services Limited
1 Montarik House
3 Bedlam Court
Gibraltar
Attn: Data Protection Officer

J. How we handle requests. If we receive a request from you to exercise any of the above rights, we may ask you to verify your identity before acting on the request to ensure that your data is protected and kept secure. We are required to respond to your request within one month of receipt of the request. However, in certain circumstances, we may take an additional two months to respond. We may be subject to EU or Member State law that restricts some of your rights primarily in order to safeguard national security, public defence, public security, the prevention, investigation, detection or prosecution of criminal offences, other important objectives of general public interest of the EU or of a Member State, the protection of judicial independence and judicial proceedings, the prevention, investigation, detection and prosecution of breaches of ethics for regulated professions, the protection of the data subject or the rights and freedoms of others and the enforcement of civil law claims.

VI. How we protect your personal data

IDT takes your privacy seriously and takes every reasonable measure and precaution to protect and secure your personal data. Our employees are trained on the importance of protecting your privacy and on the proper access to, use and disclosure of personal data. We work hard to protect you and your data from unauthorised access, alteration, disclosure or destruction and we have implemented technical, organizational and physical controls, safeguards and measures including:

- **Physical Access Controls** – to prevent unauthorized persons from gaining access to data processing systems and include secure areas and equipment security. Physical access rights and authentication controls for secure areas have been implemented and documented and will be regularly reviewed and updated by central functions. We secure data on computer servers in a controlled, secure environment.
- **Logical Access Controls** - to prevent data processing systems from being used without authorisation by way of personal login with a secure password that has to be changed periodically.

- **Data Access Controls -** to ensure that persons with system access authorisation have access only to those data they are authorized to process and use. A process has been established to ensure that data is accessed only by those persons who are required to gain access for their work. Access is regulated by way of personal login with a secure password and two factor authentication.
- **Disclosure Controls -** to ensure that personal data cannot be read, copied, altered or removed without authorisation during electronic transfer or transport or while being recorded onto data storage media. State-of-the-art data transmission techniques are used that ensure (amongst other things) that it will be possible to check the recipient of the personal data transferred. Storage and transport precautions are taken to protect data media against damage or theft.
- **Input Controls -** to ensure that it is possible after the fact to check and ascertain whether personal data have been entered into, altered or removed from data processing systems and if so, by whom. Logs are regularly evaluated by the person responsible for the system.
- **Job Controls** – to ensure that personal data is processed strictly in compliance with our instructions. We take steps to ensure that any natural person or processor acting under our authority does not process data except on instructions from us (except as otherwise required by law).
- **Availability Controls -** to ensure that personal data is protected against accidental destruction or loss, for instance by way of regular updates and storing of data on separate computer equipment or storage media.
- **Separation Controls -** to ensure that data collected for different purposes can be processed separately by way of separating the access to the data.
- **Default Controls** – to ensure that we only process your data which are necessary for each specific purpose of the processing, that we wherever possible minimize the processing of your data and that maintain transparency with regard to the functions and processing of your data.
- **Encryption Controls** – to convert data into a code to make your data unreadable by anyone who might intercept it and include using 128-bit encryption on our online pages that hold your data, the pseudonymisation of data and the use Secure Socket Layer (SSL) encrypted protection to protect data.
- **Industry Controls** – to ensure that our receipt and processing of certain payment data are in compliance with Payment Card Industry standards.
- **Monitoring Controls** – to enable us to constantly check the ongoing confidentiality, integrity, availability and resilience of our processing systems. We routinely test and evaluate the effectiveness of our technical and organizational safeguards and measures.
- **Your Online Security Controls -** You must be responsible for protecting your own personal data, and we recommend that you keep your PC or device updated with anti-virus software, treat emails with caution (remember we will never ask you to disclose personal data via email) and ensure you choose a password that can not be easily guessed.

Although we work hard to protect your data, no program is 100% secure and we cannot guarantee that our safeguards will prevent every unauthorized attempt to access, use or disclose that data. The risks that may result from our processing of your personal data include identity theft or fraud, financial loss, loss of confidentiality, unauthorised reversal of pseudonymisation, and the inability to exercise control

over your personal data. IDT maintains security and incident response plans to handle incidents involving unauthorized access to information we collect or store. If you become aware of a security issue, please contact us.

VII. Personal Information of Children

IDT does not knowingly market to or collect information from children under the age of 13 without obtaining verifiable parental consent. If you allow a child to use your device or card services, you should be aware that their personal information could be collected as described in this policy. We encourage parents to be involved in the online activities of their children to ensure that no information is collected from a child without parental permission.

Certain Program Managers that market our Cards, do so in conjunction with payment services designed to be used by children. If you are a user of such services you should also refer to the privacy policy on that Program Manager's website.

VIII. Transfers of data inside and outside the EEA

Personal data in the EU is protected by the GDPR, but some other countries may not necessarily have the same high standard of protection for your data. We transfer data outside the European Economic Area to both our affiliates in the USA as mentioned in Article IV above, and certain card processors in other non-EU EEA countries. The purpose of transferring data to such payment card processors is to facilitate the settlement of transactions performed on and by the Cards. Therefore, when you use our Services the personal data you submit may be stored on servers which are hosted in the United States, or other non-EEA countries. Where this is the case, we will take steps to ensure that those affiliates and vendors use the necessary level of protection for your data and abide by strict agreements and measures to protect your data and comply with the relevant data protection laws.

IX. Consequences of not providing your data

You are not obligated to provide us with your personal data. However, this data is necessary for us to provide you with our Services. Accordingly, we will not be able to offer some or all our Services to you and/or you will not able to use certain features or functions of our Services, without providing us with your personal data. In addition, we may need to collect personal data by law or under the terms of a contract we have with you. If you choose not to give us this data, it may delay or prevent us from meeting our obligations. It may also mean that we cannot perform services needed to maintain your Card, and could mean that we cancel a Card issued to you by us.

X. Legitimate interests

As noted in the *'How We Use Your Personal Data'* section of this notice, we often process your personal data under the legitimate interests legal basis. Where this is the case, we have carried out a thorough review and assessment to ensure that we have weighed and balanced your interests and any risk posed to you against our own interests and ensuring that are processing activities are proportionate and appropriate. Based on our assessment, we reasonably believe that our direct marketing processing activities do not pose a likely privacy risk or detriment to you or your data.

We use the legitimate interests legal basis for processing for the purposes and interests listed in the *'How We Use Your Personal Data'* section of this notice.

XI. How long we keep your personal data

IDT retains your data for only as long as is necessary for the purposes described above in *'How We Use Your Personal Data'* and we have strict review and retention policies in place to meet these obligations. We are required under applicable European and Gibraltar financial services laws to keep your certain personal information for a minimum of 10 years after which time it will be destroyed unless required to be kept for other purposes.

XII. How you can lodge a complaint or contact us

IDT only processes your personal data in compliance with this notice and in accordance with the relevant data protection regulations and laws. We will always aim to collect and use your personal data in a way meets the highest data protection standards. We take any complaints about data protection very seriously. If you wish to contact us, raise a complaint regarding the processing of your data or are unsatisfied with how we have handled your data, you can contact us in writing at:

IDT's contact information

IDT Financial Services Limited
1 Montarik House
3 Bedlam Court
Gibraltar
Email: privacy@idtfinance.com
IDT's Data Protection Officer: Giovanni Santini
IDT's Representative's Email: privacy@idtfinance.com

You have the right to lodge a complaint with the supervisory authority. The Information Commissioner's Office (ICO) may be contacted at:

Supervisory Authority contact information

Gibraltar Regulatory Authority
2nd floor
Eurotowers 4
1 Europort Road
Gibraltar
Email: info@gra.gi

Appendix 1

Subject Access Request Form

Under the General Data Protection Regulation, you are entitled as a data subject to obtain from IDT, confirmation as to whether we are processing personal data concerning you, as well as to request details about the purposes, categories and disclosure of such data.

You can use this form to request information about, and access to any personal data we hold about you. Details on where to return the completed form can be found at the end of the form.

1. Personal Details:

Data Subject's Name:		**DOB:**	___ / ___ / _____
Home Telephone No:		**Email:**	

Data Subject's Address:

Any other information that may help us to locate your personal data:

2. Specific Details of the Information Requested:

3. Representatives *(only complete if you are acting as the representative for a data subject)*

***[Please Note:** We may still need to contact the data subject where proof of authorisation or identity are required]*

Representative's Name:		**Relationship to Data Subject:**	
Telephone No:		**Email:**	

Representative's Address:

I confirm that I am the authorised representative of the named data subject:

Representative's Name: _____ **Signature:** _____

4. Confirmation

Data Subject's Name: _____ [print name]

Signature: _____ **Date:** ____ /____ /_____

5. Completed Forms

For postal requests, please return this form to:

IDT Financial Services Limited
1 Montarik House
3 Bedlam Court
Gibraltar

For email requests, please return this form to:

privacy@idtfinance.com

Attn: Data Protection Officer