Privacy Policy

Hi, we are Incard, a financial hub for digital entrepreneurs. Our technology company, Incard Ltd, offers a platform through which customers may access a variety of financial products and services offered by our partners, licensed issuers and us. We want to build a long-lasting relationship based on trust with you, so we have prepared a clear and transparent document about how we use your personal information.

We are committed to protecting and respecting your privacy.

We will:

- always keep your information safe and private;
- never sell your information; and
- allow you to manage and review marketing choices at any time.

1. WHO ARE WE?

Incard is your Data Controller

Incard is the Data Controller of your data, which means we're responsible for your personal data processed in relation to your use of the products and services accessible via the Incard Platform. Incard is a group made up of different companies, if your company is registered in the UK or you operate as a sole-trader business in the UK, you will be dealing with **INCARD LTD** and if your company is registered in one of the EEA member countries or you operate as a sole-trader business in one of the EEA countries you will be dealing with **INCARD EUROPE LIMITED**. When you visit our website and/or receive services via the Incard Platform we collect, process, use and are responsible for certain personal data about you.

When we do so,

- **INCARD LTD** is regulated under the applicable laws on the protection of personal data, privacy and electronic communications, including but not limited to The Data Protection Act 2018 (the "**DPA 2018**", the United Kingdom General Data Protection Regulation (the "**UK GDPR**") and The Privacy and Electronic Communications Regulations ("**PECR**").
- **INCARD EUROPE LIMITED** is regulated under the requirements of any applicable laws and legal acts of the Personal Data protection on the level of country where we operate as well as the General Data Protection Regulation of 27 April 2016 ("**GDPR**").

For the purposes of these laws we are responsible as a '**Data Controller**' for the processing of your personal data. If you have any queries about this Privacy Policy or how we may collect, store or use your data, please contact us by email at **support@incard.co**.

Incard is also your Data Processor in some cases

When using some of our services and products, like Incard Cards, Incard is a '**Data Processor**' and The Currencycloud Limited is a '**Data Controller**' which means we process personal data solely for the purposes of providing you with the Incard Card issued by Transact Payments Limited.

Also when we process personal data you provide to us that is related to other individuals (such as your employees or customers), we may be acting as a Data Processor. In this case Incard is a '**Data Processor**' and you are a '**Data Controller**', which means we process personal data solely for the purposes of providing you with our Incard Products and Services and based on your instructions.

In particular, when you engage with Incard Products and Services, or those of our partners, Incard will likely be acting as a Data Processor of that data.

Your personal data held in our database or Identify personal data category or categories will be stored on the servers of our hosting service providers and the hosting services providers of our services providers. Incard Ltd is managing the hosting environment for incard iOS App and incard Web App and is hence a processor of the organization which uses incard products.

Incard Ltd engaged Amazon Web Services Inc. as sub-processor in order to provide certain cloud services (eu-west-2, Europe (London) (https://aws.amazon.com/about-aws/global-infrastructure/)).

When we act as a Data Processor we are required to have a written agreement in place with you which outlines how we process the personal data we process on your behalf and that you provide to us in your capacity as Data Controller. We will let you know if you are using Incard Products and Services for which you are a '**Data Controller**' and where you shall review and enter into a Data Processing Agreement ('**DPA**') with us. By using those services, you will be deemed to have read, reviewed and agreed to our DPA with you. If you have any questions about the DPA, please get in touch with us at **dpo@incard.co**.

2. HOW WE COLLECT YOUR PERSONAL DATA?

2.1. We collect personal data from you provide when you:

- fill in any forms;
- correspond with us;
- register to use the incard app;
- open an account or use any of our services;
- take part in online discussions, surveys or promotions;
- speak with a member of our customer support team (either on the phone, through the website or through the app); or
- contact us for other reasons.

2.2. We also collect personal data from a number of different third parties, including our service partners (defined below).

Type of Third Party	Description	Collect	Share
Member of the incard Group	Our affiliated companies	✓	✓
Transact Payments	Our issuer.	✓	✓

Limited			
Payment Processing Partners and Vendors	Financial services providers, including card issuers, payment processors and banking partners to facilitate payment transactions. These third parties may be part of Open Banking, which means they may be able to send information they hold about your account and transactions to us (based on your consent).	✓	✓
Support tools and operational partners	These include analytics, search engine service providers, customer experience support platforms to optimise and improve our services, as well as subcontractors we may use to supplement our customer support resources.	x	✓
Hosting and IT Service Provider	IT vendors, including cloud storage providers, to securely store your personal data.	x	✓
Incard Card Manufacturers and Delivery Providers	Card manufacturing, personalisation and delivery companies.	x	✓
Identity and other information verification providers	We work with third parties to verify the information you provide to us, for example your identity and address.	✓	✓
Social networks and other online platforms providers	Social media sites, for the purposes of conducting market research, marketing campaigns, targeted and retargeted marketing and understanding the success of our marketing activities. These social media sites may check if you hold an account with them and, based on the characteristics they have about you, provide targeted advertising to you (for example, to show you tailored advertisements on their social media platforms,	✓	✓

	depending on your potential interest in Tide Products and Services).		
Public Data Sources	Companies House, LinkedIn and other public data sources.	✓	x
Marketing, Business Development and Sales Partners	Third parties that help us generate sales and marketing leads, and create and deliver our marketing activities.	✓	✓
Insurers and Professional Advisors		x	✓
Data Services Third Parties	Such as data analytics and insight firms, for example to test the quality of our data, to improve the effectiveness of our crime prevention controls, etc.	x	✓
Government and regulatory organisations	Government, law enforcement agencies, authorities and regulatory bodies when Tide has to comply with its legal obligations.	x	✓

2.3. Depending on the circumstances, the organisations or people who we share your personal information with will be acting as either Data Processors or Data Controllers. When we share your personal information with a Data Processor, we will ensure that we have in place contracts that set out the responsibilities and obligations of us and them, including in respect of security of personal information.

2.4. We do not sell or trade any of the personal information that you have provided to us.

3. WHAT TYPES OF DATA WILL WE COLLECT?

3.1. We have set out the general categories of personal and special data that we process and, in the case of personal and special data that we have not obtained directly from the customer, information on the source and specific categories of that data.

3.2. Incard may collect the following personal data from you:

General Category	Types of Personal Data in that category	Retention Periods
Identity information	This is information relating to your identity such as your name (including any previous names and any titles that you use), gender, marital status and date of birth	**At least five years** from the date you terminated the services save that involve any suspicious activities.
Contact information	This is information relating to your contact details such as email address, addresses, telephone numbers	**At least five years** from the date you terminated the services save that involve any suspicious activities.
Account information	This is information relating to your account with us (including username and password)	It is **no longer than 1 years after termination** of the service, save that it is involved in any suspicious activities.
Payment information	This is information relating to the methods by which you provide payment to us such as [bank account details, credit or debit card details] and details of any payments (including amounts and dates) that are made between us	**At least five years** from the last of the transactions save that it is involved in any suspicious activities.
Transaction information	This is information relating to transactions between us such as details of the goods, services and/or digital content provided to you and any returns details	**At least five years** from the last of the transactions save that it is involved in any suspicious activities.

Survey information	This is information that we have collected from you or that you have provided to us in respect of surveys and feedback	It is no longer **2 years after the survey** was completed.
Marketing information	This is information relating to your marketing and communications preferences	It is no longer than **1 years after termination**.
Website, Device and Technical Information	This is information about your use of our website and technical data which we collect (including your IP address, the type of browser you are using and the version, the operating system you are using, details about the time zone and location settings on the device and other information we receive about your device)	**At least five years** from the date you terminated the services or from the last of the transactions saved that involve any suspicious activities.

3.3. The types of personal data we collect about you may differ from person to person, depending on who you are and the relationship between us.

3.4. Incard will also collect certain very sensitive personal information that requires extra protection under data protection law 'Special Information'. We collect and hold the following types of special information about you: race, ethnic, politics, religion, trade union memberships, genetics; biometrics, health, sex life, sexual orientation.

3.5. Where we do hold special information about your then our retention periods are as follows:

Type of Special Information	**Retention Periods**
List from 3.4	At least five years from the date terminated the services save that involve any suspicious activities.

3.6. We do not collect information from you relating to criminal offenses.

4. WHY AND HOW WE USE PERSONAL INFORMATION?

4.1. So that we are able to provide you with goods and services, we will need your personal information. If you do not provide us with the required personal information, we may be prevented from supplying the goods and services to you.

4.2. We are only able to use your personal information for certain legal reasons set out in data protection law. There are legal reasons under data protection law other than those listed below; but, in most cases, we will use your personal information for the following legal reasons:

1. **Contract Reason**: this is in order to perform our obligations to you under a contract we have entered into with you;
2. **Legitimate Interests Reason**: this is where the use of your personal information is necessary for our (or a third party's) legitimate interests, so long as that legitimate interest does not override your fundamental rights, freedoms or interests;
3. **Legal Obligation Reason**: this is where we have to use your personal information in order to perform a legal obligation by which we are bound; and
4. **Consent Reason**: this is where you have given us your consent to use your personal information for a specific reason or specific reasons.

4.3. As explained in section 3 above, there are more sensitive types of personal data, which require higher levels of protection. Where we process such sensitive types of personal data, we will usually do this in the following circumstances:

1. We have your explicit consent;
2. Where it is necessary in relation to legal claims;
3. Where you have made the personal data public.

4.4. Where we rely on consent for a specific purpose as the legal reason for processing your personal information, you have the right under data protection law to withdraw your consent at any time. If you do wish to withdraw your consent, please contact us using the details set out in this notice. If we receive a request from you withdrawing your consent to a specific purpose, we will stop processing your personal information for that purpose, unless we

have another legal reason for processing your personal information – in which case, we will confirm that reason to you.

4.5. Under data protection laws, we can only use your personal information for the purposes we have told you about, unless we consider that the new purpose is compatible with the purpose(s) we told you about. If we want to use your personal information for a different purpose that we do not think is compatible with the purpose(s) we told you about, then we will contact you to explain this and what legal reason is in place to allow us to do this.

5. KEEPING YOUR INFORMATION UP TO DATE

It is important that you keep your personal information up to date. If any of your personal information changes, please contact us as soon as possible to let us know. If you do not do this, then we may be prevented from supplying the goods and services to you (for example, if you move address and do not tell us, then your goods may be delivered to the wrong address.

6. WE MAY SHARE ANONYMISED DATA

Sometimes we may anonymise personal information so that you can no longer be identified from it and use this for our own purposes. In addition, sometimes we may use some of your personal information together with other people's personal information to give us statistical information for our own purposes. Because this is grouped together with other personal information and you are not identifiable from that combined data we are able to use this.

7. WE MAY TRANSFER YOUR PERSONAL DATA OUTSIDE THE UK AND THE EEA

7.1. If any transfer of personal information by us will mean that your personal information is transferred outside of the EEA, then we will ensure that safeguards are in place to ensure that a similar degree of protection is given to your personal information as is given to it

within the EEA and that the transfer is made in compliance with data protection laws (including, where relevant, any exceptions to the general rules on transferring personal information outside of the EEA that are available to us – these are known as 'derogations' under data protection laws). We may need to transfer personal information outside of the EEA to other organisations within our group or to the third parties listed above in section 6 who may be located outside of the EEA.

7.2. The safeguards set out in data protection laws for transferring personal information outside of the EEA include:

1. Where the transfer is to a country or territory that the EU Commission has approved as ensuring an adequate level of protection;
2. Where personal information is transferred to another organisation within our group, under an agreement covering this situation, which is known as 'binding corporate rules';
3. Having in place a standard set of clauses that have been approved by the EU Commission;
4. Compliance with an approved code of conduct by a relevant data protection supervisory authority (in the UK, this is the Information Commissioner's Office (ICO);
5. Certification with an approved certification mechanism;
6. Where the EU Commission has approved specific arrangements in respect of certain countries, such as the US Privacy Shield, in relation to organisations that have signed up to it in the USA.

8. HOW WILL WE RETAIN AND DELETE YOUR PERSONAL DATA

8.1. We will only hold your personal data for as long as you are an incard customer or as long as necessary.

8.2. We may keep your personal data after you stop being a customer. The reasons we may do this are:

- To respond to a question or complaint, or to show whether we gave you fair treatment
- To establish, exercise or defend our legal claims

- To study customer data as part of our own research when this will not cause harm to your privacy and personal data protection rights
- To comply with legal rules that apply to us about keeping records or information in which case we will retain your data for a minimum of six years after your account has been terminated or longer depending on domestic laws.

8.3. We may also keep your data if certain laws that incard is subject to stipulate that we cannot delete it for legal, regulatory or technical reasons.

8.4. We have set out above the details of our retention periods for different types of data. You can find them in section 3.

9. AUTOMATED DECISION MAKING

9.1. 'Automated decision making' is where a decision is automatically made without any human involvement. Under data protection laws, this includes profiling. 'Profiling' is the automated processing of personal data to evaluate or analyse certain personal aspects of a person (such as their behaviour, characteristics, interests and preferences).

9.2. Data protection laws place restrictions upon us if we carry out any automated decision making (including profiling) that produces a legal effect or similarly significant effect on you.

9.3. We do not carry out any automated decision making (including profiling) that produces a legal effect or similarly significant effect on you. If we do decide to do this then we will notify you and we will inform you of the legal reason we are able to do this.

10. MARKETING

10.1. You may receive marketing from us about similar goods and services, where either you have consented to this, or we have another legal reason by which we can contact you for marketing purposes.

10.2. However, we will give you the opportunity to manage how or if we market to you. In any email that we send to you, we provide a link to either unsubscribe or opt out, or to change

your marketing preferences. If you have an account with us, you can login to your account and manage your preferences there too. To change your marketing preferences, and/or to request that we stop processing your personal information for marketing purposes, you can always contact us on the details set out at the beginning of this notice.

10.3. If you do request that we stop marketing to you, this will not prevent us from sending communications to you that are not to do with marketing (for example in relation to services that you have purchased from us).

10.4. We do not pass your personal information on to any third parties for marketing purposes.

11. YOUR RIGHTS UNDER DATA PROTECTION LAW

11.1. Under data protection laws, you have certain rights in relation to your personal information, as follows:

- Right to request access: (this is often called ‘subject access’). This is the right to obtain from us a copy of the personal information that we hold about you. We must also provide you with certain other information in response to these requests to help you understand how your personal information is being used.
- Right to correction: this is the right to request that any incorrect personal data is corrected and that any incomplete personal data is completed.
- Right to erasure: (this is often called the 'right to be forgotten').This right only applies in certain circumstances. Where it does apply, you have the right to request us to erase all of your personal information.
- Right to restrict processing: this right only applies in certain circumstances. Where it does apply, you have the right to request us to restrict the processing of your personal information.
- Right to data portability: this right allows you to request us to transfer your personal information to someone else.
- Right to object: you have the right to object to us processing your personal information for direct marketing purposes. You also have the right to object to us processing personal information where our legal reason for doing so is the Legitimate Interests Reason (see section 4 above) and there is something about your particular situation that

means that you want to object to us processing your personal information. In certain circumstances, you have the right to object to processing where such processing consists of profiling (including profiling for direct marketing).

11.2. In addition to the rights set out in section 9.1, where we rely on consent as the legal reason for using your personal information, you have the right to withdraw your consent. Further details about this are set out in section 4.5.

11.3. If you want to exercise any of the above rights in relation to your personal information, please contact us using the details set out at the beginning of this notice. If you do make a request, then please note:

- we may need certain information from you so that we can verify your identity;
- we do not charge a fee for exercising your rights unless your request is unfounded or excessive; and
- if your request is unfounded or excessive, then we may refuse to deal with your request.

11.4. For further data on each of those rights, including the circumstances in which they apply, see the Guidance from the UK Information Commissioner's Office (ICO) on individual rights under the GDPR .

11.5. Please note that your specific rights may vary depending on the country you are established in.

11.6. If you would like to exercise your rights, please contact us at support@incard.co or at:

Incard Ltd
71-75 Shelton Street,
Covent Garden, London,
WC2H 9JQ
United Kingdom

12. HOW DO WE PROTECT YOUR PERSONAL DATA?

12.1. incard understands the importance of safeguarding and maintaining your personal information. We will treat any personal data we process with the greatest care and security. This section explains some of the safeguards we have in place.

12.2. To keep your personal data safe and prevent unauthorised access, use, or disclosure, we employ a range of physical and technical safeguards. Electronic data and databases are stored on secure computer systems, with physical and electronic access to information controlled. Our employees are trained in data protection and information security. When our employees handle your personal data, they must adhere to our rigorous security and data protection standards.

12.3. While we take all reasonable precautions to protect your personal data from unauthorised access, we cannot guarantee that it will be secure during transfer to our app, website, or other services by you. For all of our app, web, and payment-processing services, we employ HTTPS (HTTP Safe), where the communication protocol is secured by Transport Layer Security for secure communication over networks.

12.4. Although we take all reasonable precautions to protect your personal data from unauthorised access, we cannot guarantee that it will be secure when transferred to our app, website or other services by you. For all our application, website and payment processing services, we use HTTPS (HTTP Safe), where the communication protocol is secured by Transport Layer Security for secure communication over networks.

13. HOW TO CONTACT US AND HOW TO COMPLAIN?

13.1. incard has appointed a specified person as the data protection officer ("**the DPO**") who you can contact at dpo@incard.co or at INCARD LTD, 71-75 Shelton Street, Covent Garden, London, United Kingdom, WC2H 9JQ.

13.2. You also have the right to complain to the regulator. The supervisory authority in the UK is the Information Commissioner's Office (ICO). You can find out how to report a concern on their website – https://ico.org.uk/.

14. OUR KEY PARTNER THE CURRENCYCLOUD LIMITED IS ALSO A DATA CONTROLLER

14.1. In addition to the above ways in which we process and share your personal data, Incard also shares this data with companies who are integral in allowing us to offer our products and services to customers.

14.2. The Currencycloud Limited becomes Data Controllers in relation to your personal data shared with them for the purpose of issuing and storing Electronic Money and issuing debit cards pursuant to a license from VISA International Incorporated. This means that if you would like to exercise any of the rights afforded to you by the personal data protection laws applicable to your case, these companies must be contacted separately from Incard. The following ways describe how and why we share your data with The Currencycloud Limited:

Who is The Currencycloud Limited and why do they handle my data?

The Currencycloud Limited, also known as 'CC' is a global payment platform. CC is authorised by the FCA under the Electronic Money Regulations 2011 (register reference 900199) for the issuing of Electronic Money and registered in England & Wales with a registered office at 100 New Bridge Street, London, United Kingdom, EC4V 6JA No. 06323311.

CC is a Data Controller in relation to the issuing and storing of the Electronic Money, your card and all necessary activities relating to the operation of the card: allowing you to receive, activate and use your Card. The processing of your personal data is necessary for the performance of your contract for the issue and operation of cards and is necessary for compliance with legal and regulatory obligations applicable to CC. CC does not use your

personal data for marketing purposes and will not share your personal data with third parties for marketing purposes.

What personal data does CC process?

CC will collect some personal data about you and the user of the Card in connection with the Card application and the use of the Card. For information regarding how CC process personal data, please see their Privacy Notice.

How do I contact CC?

Address:

The Currency Cloud Limited, 1st Floor Stewardship Building, 12 Steward Street, London, E1 6FQ, United Kingdom.

Attention to: Customer Service

Email: info@currencycloud.com

Telephone: +44 203 326 8173

Attention to: the Data Protection Officer

Email: dpo@currencycloud.com

15. THIRD PARTIES WEBSITE

Our website may contain links to third-party websites. If you click and follow those links, then these will take you to the third-party website. Those third-party websites may collect personal information from you and you will need to check their privacy notices to understand how your personal information is collected and used by them

16. HOW TO WITHDRAW YOUR CONSENT OR OPT-OUT OF PROCESSING?

You can withdraw your consent to our processing of your data at any time. Please contact us if you want to do so at support@incard.co.

This will only affect the way we use data when our basis for processing your data is your consent. See the section ‘Your Rights’ and more specifically your right to restricting use of your data.

You may also opt out of some forms of data processing we are conducting, such as:

- Marketing, including email, phone and SMS marketing.
- Social media and targeted marketing, including retargeting and curated audiences.
- Non-essential cookie collection on Our Website. You may be unable to opt out of ‘necessary’ cookies as discussed above.
- Non-essential profiling and automated decision-making, including those activities undertaken for marketing purposes.

If you withdraw your consent and/or opt-out, we may not be able to provide certain products or services to you. If this is so, we will tell you. You then have the option to give us your consent again if you want to access our products or services.

17. SECURITY

We have put in place appropriate security measures to prevent your personal data from being accidentally lost, used, changed, shared or accessed in a way it shouldn’t be. We will employ adequate technical and organisational security measures to protect your personal data. These methods include:

- The pseudonymisation and encryption of personal data, where possible.
- Ensuring the ongoing confidentiality, integrity, availability and resilience of processing systems and services via role-based access controls, confidentiality undertakings of our staff, etc.
- The ability to restore the availability and access to personal data quickly in the event of or technical incident.
- A process for regularly testing, assessing and evaluating the effectiveness of our technical and organisational measures.

We will also limit access to your personal data to employees, agents, contractors and other third parties who have a strict need to see it in order to perform their business functions. They will only process your personal data on a 'need-to-know' basis, pursuant to our instructions and they will keep your personal data confidential.

We have put in place procedures to deal with any suspected personal data breach and will let you and any applicable regulator know of a breach when we have to by law.

18. KEEPING YOUR DATA ACCURATE

We will use reasonable efforts to ensure that your personal data is accurate, complete and up-to-date. Please ensure you notify us without undue delay of any changes to the personal data that you have provided to us by updating your details on the Tide Platform or by contacting us at the details provided in this Privacy Policy.

Schedule 1

Key Definitions

Data Protection Laws: the Data Protection Act 2018 and the General Data Protection Regulation ((EU) 2016/679) (the GDPR) and such other laws as may be applicable from time to time, including any replacements.

GDPR: the General Data Protection Regulation ((EU) 2016/679).

Data Controller: under UK data protection law, this is the organisation or person responsible for deciding how personal information is collected and stored and how it is used.

Data Processor: a Data Controller may appoint another organisation or person to carry out certain tasks in relation to the personal information on behalf of, and on the written instructions of, the Data Controller. (This might be the hosting of a site containing personal data, for example, or providing an email-marketing service that facilitates mass distribution of marketing material to a Data Controller's customer base.)

Personal Information: in this privacy notice, we refer to your personal data as 'personal information'. 'Personal information' means any information from which a living individual can be identified. It does not apply to information that has been anonymised.

Special Information: certain very sensitive personal information requires extra protection under data protection law. Sensitive data includes information relating to health, racial and ethnic origin, political opinions, religious and similar beliefs, trade union membership, sex life and sexual orientation and also includes genetic information and biometric information.