TRUEPOS
PAYMENT SOLUTIONS

Our commitment to you and the protection of your data at Truepos Payment Solutions.

As of May 25, 2018, the 'General Data Protection Regulation' or GDPR is enacted across all Member-states of the European Union and the European Economic Area. GDPR aims to harmonise the different data protection laws across the Member-states, leading to more standardised protections for all European citizens. At Truepos Payment Solutions we welcome this regulatory change because we have always strived to provide our clients with the highest protection of their personal data.

Organisational Readiness Truepos Payment Solutions.

The protection of our customers' personal data is of utmost importance to us. In the last year, we have worked tirelessly to ensure all GDPR compliance requirements were met well in advance. We also follow all practices in this area and all issued guidelines of the regulatory bodies to adapt our protection measures constantly and adequately.

Data Protection Officer, Privacy Team and GDPR Training

All our employees have undergone GDPR training, overseen by our on-site Privacy Team, Compliance Department and our outside privacy consultants. Each new employee must participate in a mandatory training session related to privacy regulations and best practices. New training sessions are carried out annually thereafter for all employees. We have appointed our Data Protection Officer (DPO), who also acts as the Privacy Team leader, in accordance with the requirements of GDPR.

Internal policies

The company's internal policies are updated in accordance with the new GDPR requirements.

The data we collect

The personal data we collect and process is described in detail in our Privacy Policy. We process the personal data on the basis of different grounds, defined by GDPR – legal obligations, for the purposes of concluding and/or executing a legal relationship, legitimate interest and based on clients' consent.

How we use the collected data

We use, store, and process the personal information to provide, understand, improve, and develop our services, create and maintain a secure environment, pursue our legitimate interests and comply with our legal obligations. For detailed information please check our Privacy Policy.

Truepos Payment Solutions clients and their related personal data

All of our clients are legal entities (companies/corporations). The data about the sole traders is personal data under GDPR. The rest of the corporations/companies are not data subjects under the law. However, we are obliged to verify the identity of the business owner/authorised user, who is opening the Account (in case of company or other entity, referred to as "user opening the Account"). We are processing the personal data about this business owner/authorised user. **The information regarding the company (with the exception of sole traders), including its risk profile and due diligence checks is not regulated by GDPR.**

Why are we taking pictures of an entity's authorised persons and their ID documents and is it GDPR-compliant?

Truepos Payment Solutions service is designed for business purposes and may be used by individuals or entities. In case you are registering for and/or using our services on behalf of an entity we will treat you as authorised person and you may be obliged to disclose to us personal data of the legal representatives, the employees, the agents, the beneficial owners or any other third-party related to the entity.

In accordance with our legal obligations under the relevant Anti-money laundering and anti-terrorism financing regulations (or AML/CFT laws), we are obliged to verify our customer's identity or the identity of the authorised user who is opening the Account.

We are bound by the law to identify and verify the owner of the Account (an authorised person from the company) and since the individuals are not always able to upload the required information on their own, we do it instead. We do this for our clients' convenience.

The AML/CFT laws, in broad terms, require financial institutions and other entities that are at risk of being used as a tool to launder money or finance terrorism, to:

1. identify their clients, which means that the obliged entity must ask the client to provide his/her personal details.
2. verify their identity, which means that the obliged entity must "check" that the personal details of the person are not falsified, forged, stolen or similar.

Data Protection Impact Assessment

We have carried out a detailed review of all our data processing activities, by product and by department. We have analysed the grounds for processing, retention periods, technical and legal safeguards for our client's rights and freedoms and we have ensured that any data processing activity that we carry out is 100% compliant with the law.

Our retention periods

Please be aware that, as a financial institution, we are required by the Payment Services Directive and money laundering legislation to keep client's data for a period of 5 years after the termination of the contract/account of our customer.

Correction (rectification) of client's personal data

Our customers can **send us a request to correct inaccurate or incomplete personal information via email to** help@truepos.ie

Data Access

Our clients have the **right to receive a copy of the data we hold for them at any time. The request can be sent via e-mail to** help@truepos.ie.

Data Deletion

We generally retain clients' personal information for as long as is necessary for the performance of the contract between them and us and to comply with our regulatory obligations.

In case the regulatory retention periods have expired, we diligently delete clients' personal information from our systems. The request for deletion can be sent via e-mail to help@truepos.ie

For additional information, please check our Privacy Policy.

Data transfer as our clients' right

Our clients have the right to receive a copy of their personal data in a structured, commonly used, machine-readable format that supports re-use. They can transfer their personal data from one controller to another and/or have the personal data transmitted directly between controllers without hindrance.

Consent withdraw and restriction of personal data processing

Where our clients have provided their consent to the processing of personal information by us, they may withdraw the consent at any time by changing the Account settings or by sending a communication to us specifying which consent they are withdrawing. Please note that the withdrawal of consent does not affect the lawfulness of any processing activities based on such consent before its withdrawal.

Data subjects' rights and legal entities

Please be informed that corporations are not data subjects under GDPR. Business owners who use Truepos Payment Solutions services and have business accounts can exercise their rights, but only regarding their personal data (or the personal data of the authorised person). The information regarding their company, including its risk profile and due diligence checks is not regulated by GDPR.

With whom we share personal data

We may share personal data with members of the Premier Utilities LTD Group of companies as we aim to provide the services our clients have requested and in order to help detect and prevent potentially illegal and fraudulent acts and other violations of our policies. We also may share personal information with third party service providers that support us in providing Truepos Payment Solutions, products and/or Platform with functions at our decision and our behalf. For more details, please see section 3 of our Privacy Policy.

Children and our services

Our services are not designed to individuals under the age of 18, unless we have expressly specified so in our Privacy Policy or other legal document. If we obtain actual knowledge that we have collected Personal Data from an individual under the age of 18, we will promptly delete it, unless we are legally obligated to retain such data.

Reviews of Vendors and Partners

All our current vendors have been reviewed to ensure they meet security and privacy requirements defined by GDPR. To maintain assurance, these reviews will be conducted for all incoming vendors. **Where we transfer, store and process personal information outside of the** European Economic Area **we guarantee that appropriate safeguards are in place to ensure an adequate level of data protection**.

Where we deal with entities outside the EEA, we always require our vendors to be either registered under Privacy Shield mechanisms (or similar) or to provide us with a review of their appropriate privacy safeguards.

Encryption and storage of personal data

We take the responsibility to ensure that your personal information is secure, kept in an encrypted from on servers, collocated in Special data centres in Class A jurisdictions in Europe. To prevent unauthorised access or disclosure of information we maintain physical, electronic and procedural safeguards that comply with applicable regulations to guard non-public personal information.

Incident response

Our Incident Response procedures have been designed and tested to ensure potential security events are identified and reported to appropriate personnel for resolution, personnel follow defined protocols for resolving security events, and steps for resolution are documented and reviewed by our Security Team on a regular basis. Additionally, we're working to update these policies and procedures to include breach notification if and when a security incident involves the loss of or unauthorized use of personal identifiable information (PII).