E-commerce site used to provide payment services and advice for commercial website operators

Legislation and Standards

Regulations of Online Payments

All websites providing online payments services, must comply with a number of regulations in order to protect the consumers and reduce fraudulent transactions. Some of the major regulations are:

- Payment Card Industry Data Security Standard (PCI DSS).

- Card Networks (Mastercard, Visa, Discover, American Express) guidelines and practises.

- EU Revised Payment Services Directive (PSD2).

- UK's Financial Conduct Authority (FCA).

- Know Your Customer (KYC).

In order to successfully evaluate if the website complies with these regulations, additional help will be required from a legal team. Basic transactional security steps can be checked, such as if a 3D Secure authentication protocol is enforced and if a statement on consumer rights is present.

Further inspection can be provided by hiring a Regtech company. Regtech companies provide support with the compliance of all existing regulations and assure continuous compliance.

Personal Data Privacy

Depending on where the website provides its services, certain data protection regulations may apply:

- Europe = General Data Protection Regulation (GDPR)
- UK = Data Protection, Privacy, and Electronic Communications (DPPEC)
- Brazil = General Data Protection Law
- Canada = Personal Information Protection and Electronic Documents Act (PIPEDA)
- South Africa = Protection of Personal Information Act (POPIA)

In order to successfully evaluate if the website complies with the data protection regulations, help from a legal department is required. However, at the most basic level, the website must provide a data protection disclaimer including a note on what data are you collecting, who is collecting the data, where are they stored and why and how will they be used.

Assumptions

- Employees show an ethical behaviour towards the data they can access.
- All servers and communication protocols are encrypted.
- The data stored are not accessible from third-parties.
- Frequent audits are performed.