



GDPR COMPLIANCE

We are protecting personal data

www.etzpayments.com

GDPR – IN A NUTSHELL: PROTECTING PERSONAL DATA IS KEY

All organisations (worldwide) offering goods and services to EU residents, must comply with the EU's General Data Protection Regulations ("GDPR"). Compliance must be in place by 25th May 2018. The purpose of the GDPR is to protect individuals' personal data, and to ensure that individuals have full control over the handling of their personal data. This means that there will be transparency on how individuals' data is handled – from collection, to processing and transfer. Strict processes must be in place to ensure that personal data is securely stored and used, with adequate reporting and record management. Any systems in place must meet the criteria of 'privacy by design and data protection by default'.

Obligations

Organisations are required to obtain consent of every individual whose personal data they handle.

Prohibitions

Organisations are prohibited from profiling sensitive personal data without explicit consent of individuals, and they are also prohibited from profiling or monitoring individuals' personal data without explicit consent.

Rights

Individuals have new rights to enable them to control how their data is handled. These comprise of the:

- Right to request access to your personal data.
- Right to request correction of your personal data.
- Right to request erasure of your personal data.
- Right to object to processing of your personal data.
- Right to request restriction of processing your personal data.
- Right to request transfer of your personal data.
- Right to withdraw consent to processing your personal data.

GDPR – IN A NUTSHELL: 5 key changes

PRINCIPLES

- Consent not coerced
- Profile prohibition
- Special data prohibition

ACCOUNTABILITY

- Code of conduct and certification
- Data breach notification within 72 hours
- Security of data (lists security measures)
- Data processors have statutory obligation to report data breach
- Appointment of DPR (Data Protection Officer) - SMEs exempt
- Privacy by design (by using pseudonymisation)
- DIPA (Data Protection Impact Assessment - for "high risk" processing)

ENFORCEMENT & REMEDIES

- Fines: 2% of global annual turnover or €10,000,000 - whichever is greatest
- Fines: 4% of global annual turnover or €20,000,000 (serious infringements) - whichever is greatest
- Joint liability of controllers and processors
- Class action

TRANSPARENCY & RIGHTS

- Transparency emphasis
- Mandatory list to appear in data protection policies
- Subjects rights: access, rectification, erasure, objection
- Right to data portability (receive data in a machine readable format for onward transmission)

INTERNATIONAL TRANSFERS

- Prohibition on transferring data to "non-adequate" countries
- Binding corporate rules and standard contract clauses are valid instruments to comply with data transfer restrictions

ETZ as a data processor adheres to GDPR

As a data processor, ETZ is fully committed to ensuring that our systems adhere to the strict requirements of the GDPR, so that we, as a business, remain a trusted partner, and service provider.

T: 0800 311 2266

W: www.etzpayments.com

