GDPR for E-Commerce Checklist

PrestaShopCompliance.com
EU compliance for merchants

Data protection basics for online shops

Establish a lawful basis

Under the GDPR (Regulation 2016/679), every processing activity needs a lawful basis. Decide the basis before you process, not after.

- [ ] Map each processing activity to a lawful basis
- [ ] Use contract necessity for order fulfilment
- [ ] Use consent for marketing where required, kept separate from purchase
- [ ] Document the basis you rely on for each purpose

Provide a clear privacy notice

You must tell people how you use their data in a concise, transparent and accessible way.

- [ ] Identify who you are and how to contact you
- [ ] Explain the purposes and lawful bases for processing
- [ ] State retention periods and who data is shared with
- [ ] Describe the rights available to data subjects

Support data-subject rights

Customers can exercise rights over their data, and you must be able to respond within the required timeframes.

- [ ] Have a process to handle access requests
- [ ] Enable correction and erasure where applicable
- [ ] Handle objections and restriction requests
- [ ] Support data portability for relevant data

Secure personal data

You must protect data with appropriate technical and organisational measures.

- [ ] Encrypt data in transit and where appropriate at rest
- [ ] Restrict access to personal data on a need-to-know basis
- [ ] Keep software, plugins and platforms up to date
- [ ] Apply strong authentication for administrative access

Manage processors and transfers

Third parties that process data on your behalf must be governed by contracts, and international transfers need safeguards.

- [ ] Put a written processor contract in place with each supplier
- [ ] Check payment, hosting and marketing tools are covered
- [ ] Identify any transfers of data outside the EU or EEA
- [ ] Ensure an appropriate transfer safeguard is in place

Keep records and prepare for breaches

Accountability means documenting your processing and being ready to respond to incidents.

- [ ] Maintain records of processing activities
- [ ] Have a breach detection and response procedure
- [ ] Be ready to notify the authority within 72 hours where required
- [ ] Notify affected individuals when the risk is high

> This checklist is general guidance and not legal advice. Obligations under Regulation 2016/679 depend on your circumstances; seek specialist advice for complex processing.