COMPLICO CONSULTING

Regulatory Compliance & Data Protection

Basic GDPR Compliance Guidelines

Do’s and Don’ts for Businesses Operating in the European Union

This document provides general guidance for businesses that process personal data of individuals located in the European Union (EU). It is intended for informational purposes only and does not constitute legal advice.

1. What is GDPR?

The General Data Protection Regulation (GDPR) is the European Union’s data protection law designed to protect the privacy and personal data of EU individuals.

Who does it apply to?

If your business sells products or services to EU customers, operates a website accessible in the EU, tracks user behavior, or processes EU personal data, you may be subject to GDPR obligations.

Examples of personal data include: names, email addresses, phone numbers, IP addresses, shipping addresses, payment information, and customer account details.

2. GDPR Compliance – Important DO’s

DO Have a Privacy Policy

Your website should clearly explain what data you collect, why you collect it, how long you keep it, and who users can contact regarding privacy matters. The privacy policy should be easy to access and written in clear language.

DO Collect Only Necessary Data

Only collect personal data that is genuinely needed for your business activities. Example: Collect shipping address for deliveries. Do not request unnecessary sensitive information.

DO Keep Customer Data Secure

Businesses should take reasonable technical and organizational measures to protect personal data, including strong passwords, restricted access, secure servers, antivirus protection, and encrypted connections (HTTPS).

DO Respond to Customer Requests

EU individuals may request access to their data, correction of inaccurate data, deletion of data, or withdrawal of consent. Such requests should be handled without undue delay.

DO Use Lawful Marketing Practices

Before sending marketing emails: obtain valid consent where required, provide an unsubscribe option, and respect opt-out requests.

DO Maintain Records of Processing

Businesses should maintain internal records describing what personal data is processed, purposes of processing, data recipients, and retention periods.

DO Appoint an EU Representative if Required

Non-EU businesses targeting EU customers may be required to appoint an EU Representative under Article 27 GDPR. Representative details should be included in your privacy policy.

3. GDPR Compliance – Important DON'Ts

DON'T Collect Data Without Purpose

Avoid collecting personal information that is unnecessary for your services or operations.

DON'T Share Customer Data Improperly

Do not sell, share, or transfer personal data to third parties without a lawful basis or proper safeguards.

DON'T Ignore Data Breaches

If customer data is lost, hacked, or exposed: investigate immediately, secure affected systems, and assess whether notification obligations apply.

DON'T Use Pre-Ticked Consent Boxes

Consent should be freely given, specific, informed, and clearly affirmative. Pre-selected checkboxes may not be compliant.

DON'T Store Data Forever

Personal data should not be kept longer than necessary. Businesses should establish reasonable retention periods.

DON'T Mislead Customers

Privacy notices and cookie banners should clearly explain what data is collected, why it is collected, and how it is used. Avoid misleading or hidden disclosures.

4. Website and E-Commerce Recommendations

Businesses operating websites or online stores should consider:

- HTTPS/SSL security,
- GDPR-compliant cookie banners,
- updated privacy policies,
- secure payment providers,
- limited employee access to customer data.

5. Consequences of Non-Compliance

Failure to comply with GDPR may result in customer complaints, regulatory investigations, reputational damage, financial penalties, or restrictions on data processing activities.

6. Final Recommendation

GDPR compliance is an ongoing responsibility. Businesses should regularly review privacy policies, internal procedures, marketing practices, and data security measures. Where necessary, businesses should seek professional legal or compliance advice.

Complico Consulting GmbH
Bahnhofstr 12, 63549, Ronneburg, Germany
VAT: DE459923379 | +49 160 7959362 | info@complicoconsulting.com | www.complicoconsulting.com