COMPLICO CONSULTING

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 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: names, email addresses, phone numbers, IP addresses, shipping addresses, payment info, account details.

2. GDPR Compliance – DO's

DO Have a Privacy Policy

Explain what data you collect, why you collect it, how long you keep it, and who to contact. Must be easily accessible and in clear language.

DO Collect Only Necessary Data

Only collect personal data genuinely needed (e.g., shipping address for deliveries). Do not request unnecessary sensitive info.

DO Keep Customer Data Secure

Take technical/organizational measures: strong passwords, restricted access, secure servers, antivirus, and encrypted connections (HTTPS).

DO Respond to Customer Requests

EU individuals may request access, correction, deletion, or withdrawal of consent. Handle requests without undue delay.

DO Maintain Records & Represent

Maintain internal records of what data is processed and why. Non-EU businesses targeting EU customers may need an EU Representative (Article 27).

3. GDPR Compliance – DON'Ts

DON'T Collect Data Without Purpose

Avoid collecting personal information that is unnecessary for your services.

DON'T Share Improperly

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

DON'T Ignore Data Breaches

If exposed: investigate immediately, secure systems, and assess notification rules.

DON'T Use Pre-Ticked Consent

Consent must be freely given, specific, and affirmative. No pre-selected boxes.

DON'T Mislead or Store Forever

Establish retention periods. Ensure privacy notices clearly explain data usage without hiding details.

4. Web & E-Commerce

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

5. Consequences of Non-Compliance

May result in customer complaints, regulatory investigations, reputational damage, financial penalties, or data processing restrictions.

6. Final Recommendation

Compliance is an ongoing responsibility. Regularly review policies, procedures, and security. Seek professional advice when necessary.

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