Gap Analysis

Dhia Gabtni

January 5, 2025

DE Shop GmbH

GDPR

Abstract

This document presents a **GDPR** compliance gap analysis for **DE Shop GmbH**, a fictional mid-sized e-commerce company based in Berlin, Germany. The objective of this project is to simulate a realistic consulting engagement to identify gaps in **GDPR** compliance and recommend actionable solutions. By conducting this analysis, the author aims to deepen their understanding of cybersecurity consulting practices and regulatory frameworks, specifically focusing on **GDPR**.
The report follows a structured approach, starting with an overview of the fictional organization and its data handling practices, progressing to the identification of compliance gaps, and concluding with practical recommendations. This exercise is designed as a hands-on learning project to showcase key skills in compliance assessment, risk management, and strategic recommendations for regulatory alignment.

As a personal project, this analysis reflects hypothetical scenarios and assumed practices, making it an educational exploration of the challenges and opportunities within the cybersecurity consulting space.

Table of Contents

Description of DE Shop GmbH Practices 5

1. General Overview 5
2. Data Collected 5
3. IT Infrastructure 5
4. Policies and Procedures 5
5. Employee Training and Awareness 5
6. Vendor Management 5

Scope and Methodology 6

1. Scope 6
2. Methodology 6

Key Findings 7

1. Privacy Policy and Transparency 7
2. Cookie Consent 7
3. Data Minimization 7
4. Data Encryption 7
5. Access Control 7
6. Data Retention 7
7. Data Breach Response 7
8. Vendor Compliance 7
9. Data Subject Requests 8
10. Employee Training 8
11. Cross-Border Data Transfers 8

Risk Assessment 9

1. Risk Categorization Framework 9
2. Table of Findings 9
3. Explanation of Prioritization 9

Recommendations 10

1. Short Term Solutions 10
2. Long Term Solution 10
3. Prioritization 11
4. Roadmap Suggestion 11

Conclusion 12

1. Recap of the Analysis 12
2. Importance of Recommendations 12
3. Next Steps 12

Appendices 12
1. Examples 12
References 13
1. Regulation and Standards 13
2. Templates and Frameworks 13
3. Supporting Articles and Case Studies 13

Table of Figures

Table 1 Table of Findings 9
Table 2 Table of Priorities 11
Table 3 Table of Tasks 11

Description of DE Shop GmbH Practices

1. General Overview

DE Shop GmbH is a Berlin-based e-commerce company specializing in home goods. It serves customers across the EU and processes personal data for order fulfillment and marketing campaigns.

2. Data Collected

Personal data includes:

- Names, email addresses, billing and shipping addresses, and purchase history.
- Optional data such as phone numbers collected during checkout.
- Cookies are used for tracking user behavior and analytics, but no consent mechanism is in place.

3. IT Infrastructure

Databases

- Customer data is stored in an on-premises MySQL database.
- Data is stored in plain text with no encryption.

Cloud Services:

- Cloud storage (via AWS) is used for backups.
- Marketing campaigns are conducted using third-party email platforms like Mailchimp

Access Control:

- Employees access the MySQL database directly without role-based access restrictions.

4. Policies and Procedures

- **Privacy Policy:**
  - The privacy policy on the website is outdated and lacks key details required by GDPR.
- **Breach Response:**
  - No formal breach response plan exists.
- **Data Retention**
  - Customer data is stored indefinitely without periodic review.

5. Employee Training and Awareness

- Employees are not trained in GDPR principles or data protection best practices

6. Vendor Management

- Vendors providing storage and marketing services are used without formal GDPR compliance assessments.

Scope and Methodology

1. Scope

The scope of this analysis focuses on **DE Shop GmbH**’s data processing practices in relation to **GDPR** requirements. Key evaluation areas include customer data collection, storage, security, transparency, consent mechanisms, breach response procedures, and third-party vendor compliance. The analysis does not extend to specific operational workflows or non-customer-facing processes.

2. Methodology

The analysis was conducted using a GDPR compliance checklist derived from key articles of the regulation, including Articles:

- Article 5 that establishes principles like:
  - **Lawfulness, fairness, and transparency**
  - **Purpose limitation**
  - **Data minimization**
  - **Accuracy**
  - **Storage limitation**
  - **Integrity and confidentiality**
- Article 7: **Conditions for Consent**
- Articles 12-22: **Rights of Data Subjects**
  - **Right to Access** (Article 15)
  - **Right to Rectification** (Article 16)
  - **Right to Erasure** (Article 17)
  - **Right to Data Portability** (Article 20)
  - **Right to Object** (Article 21)
- Article 28: **Processor Obligations**
- Article 32: **Security of Processing**
- Articles 33–34: **Data Breach Notifications**
  - **Obligation to notify the supervisory authority in case of data breach** (Article 33)
  - **Obligation to notify the individuals in case of data risk** (Article 34)
- Article 44: **Transfers of Personal Data**

These articles were picked by the author for the gap analysis due to their relevance and applicableness in this scope. Organizational practices were assessed against these standards, and gaps were identified. Each gap was evaluated based on its likelihood of occurrence and potential impact, leading to a risk categorization framework. The recommendations are prioritized based on this evaluation.

Key Findings

1. **Privacy Policy and Transparency**

   DE SHOP GmbH’s website lacks a **GDPR**-compliant privacy policy that clearly outlines how personal data is collected, processed, and stored.
   No clear communication about users' rights under **GDPR**, such as access, rectification, or deletion of their data.

2. **Cookie Consent**

   The website does not implement a cookie consent banner or mechanism to obtain user consent before placing tracking cookies.
   Users cannot manage or revoke consent for cookies once given.

3. **Data Minimization**

   The company collects more personal data than necessary (e.g., collecting phone numbers for non-essential purposes).

4. **Data Encryption**

   Customer data stored in the company’s MySQL database is not encrypted at rest or in transit.

5. **Access Control**

   Weak access controls for internal systems allow employees broad access to sensitive customer data without a clear need.

6. **Data Retention**

   The company has no defined data retention policy, leading to indefinite storage of customer data, even after it is no longer needed.

7. **Data Breach Response**

   There is no documented data breach response plan, delaying the ability to meet **GDPR**’s 72-hour breach notification requirement.

8. **Vendor Compliance**

   Third-party vendors (e.g., cloud storage, email marketing platforms) are not formally assessed for GDPR compliance.

9. Data Subject Requests

The company has no system for handling data subject requests (DSRs), such as access or deletion requests.

10. Employee Training

Employees handling customer data have not received GDPR-specific training.

11. Cross-Border Data Transfers

The company transfers personal data to processors outside the EU without verifying adequate safeguards (e.g., Standard Contractual Clauses).

Risk Assessment

1. Risk Categorization Framework

Using a simple **Likelihood x Impact** matrix

- **Likelihood:** How likely is the issue to cause a problem? (Low, Medium, High)
- **Impact:** What is the severity of the problem if it occurs? (Low, Medium, High)
- **Risk Level:** Derived by combining likelihood and impact (Low, Medium, High)

2. Table of Findings

ID	Description	Likelihood	Impact	Risk Level
1	Privacy Policy: Missing details	Medium	Medium	Medium
2	Missing Cookie Consent Banner	Medium	Medium	Medium
3	Excessive Data Collection	Low	Medium	Low
4	Data Encryption	High	High	High
5	Weak Access Controls	High	High	High
6	Undefined Data Retention Policy	Medium	Medium	Medium
7	No Breach Response Plan	Medium	High	High
8	Vendor Compliance Oversight	Low	Medium	Low
9	No Data Subject Request Process	Medium	Medium	Medium
10	Lack of Employee Training	Medium	Medium	Medium
11	Cross-Border Transfer Issues	Medium	High	High

Table 1 Table of Findings

3. Explanation of Prioritization

Although failing to comply with regulatory requirements, such as in the case of a missing cookie consent banner (Gap ID **2**), may result in fines that would severely hinder small to medium business’s continuity which in turn makes the impact level much greater. Due to the lack of context, the gaps related to data encryption, access controls, and breach response are categorized as high risk because of their potential to, not only result in severe financial loss, but also customer distrust, and other regulatory penalties. These issues should be addressed immediately to mitigate risks.

Recommendations

1. Short Term Solutions

- Implement a Cookie Consent Banner on the website that:
    - Clearly informs users about the types of cookies used
    - Allow users to accept or reject the cookies
    - Provides an option to manage or revoke cookies

- Update the privacy policy to include
    - Details about data collection, processing and retention
    - Users' **GDPR** rights (e.g., access, rectification, deletion)
    - Contact information for data protection inquiries

- Develop a Data Breach Response Plan that includes:
    - Steps for detecting and responding to breaches
    - Procedures for notifying authorities within 72 hours
    - Guidelines for informing individuals if necessary

2. Long Term Solution

- Encrypt Customer Data:
    - Implement encryption for all customer data stored in databases (at rest) and during transmission (TLS)

- Define a Data Retention Policy that:
    - Specifies retention periods for different data types.
    - Regularly reviews and deletes data no longer needed

- Train Employees on **GDPR**
    - Educating employees on **GDPR** principles
    - Ensure they understand their roles in maintaining compliance

- Implement Role-Based Access Control
    - Restrict database access based on employee roles and responsibilities to minimize unnecessary access to sensitive data

3. Prioritization

Priority	Recommendation
High	Implement Cookie Consent Banner
High	Update the Privacy Policy
High	Develop a Data Breach Response Plan
Medium	Encrypt Customer Data
Medium	Define a Data Retention Policy
Medium	Train Employees on **GDPR**
Low	Implement Role-Based Access Control

Table 2 Table of Priorities

4. Roadmap Suggestion

This roadmap outlines a structured approach to addressing the identified findings, detailing responsibilities, required resources, and expected timeframes for each task.

Task	Responsibility	Resources	Timeframe
Cookie Consent Banner	Web Dev Team	GDPR Plugins	1 Month
Privacy Policy Update	Legal & Compliance	Legal Consultant	2 Weeks
Data Breach Response Plan	IT Security Team	Incident Response Template	1 Month
Customer Data Encryption	IT Security Team	Encryption Software	3 Months
Data Retention Policy	Legal & Compliance	Legal Team, Policy Drafting Tools	3 Months
GDPR Training	HR & Compliance	External Trainer or E-Learning Platform	6 Months
Role-Based Access Control	IT Security Team	Access Management Tools	6 Months

Table 3 Table of Tasks

Conclusion

1. Recap of the Analysis

This **GDPR** compliance gap analysis for **DE Shop GmbH** identified critical areas where the organization’s data protection practices fall short of regulatory requirements. Key gaps include missing cookie consent mechanisms, unencrypted customer data, and a lack of formal breach response procedures.

2. Importance of Recommendations

Implementing the recommendations will not only ensure compliance with GDPR but also enhance the organization’s overall data security posture, protecting customer trust and reducing the risk of regulatory penalties.

3. Next Steps

DE Shop GmbH should prioritize high-risk areas such as implementing a cookie consent mechanism and encrypting customer data while laying the groundwork for long-term improvements like employee training and role-based access controls. Proactive action will position the organization as a responsible and compliant entity in the competitive e-commerce space.

Appendices

In this section of the gap analysis supplementary materials are provided to enhance the report and assist in taking the steps needed to reach compliance.

1. Examples

Examples include but are not limited to:

- Tailored **GDPR** compliance checklist
- Supporting diagrams and visuals
  - Data flow diagrams or charts that explain how data is collected, processed, and stored
  - A visual representation of the current data handling processes
- References or links to **GDPR** articles and frameworks
- Templates for policies and plans

References

1. Regulation and Standards

- Regulation (EU) 2016/679 (General Data Protection Regulation): Full text available at https://eur-lex.europa.eu

2. Templates and Frameworks

- Risk Assessment Matrix: Based on ISO 31000 Risk Management Guidelines

3. Supporting Articles and Case Studies

- “Google fined €50 million by French data regulator over GDPR violations.” Source: BBC News, January 21, 2019. Available at https://www.bbc.com
- “GDPR Fines and Enforcement Tracker,” available at https://www.enforcementtracker.com