



COMPLIANCE
PARTNERS

SAMPLE

GDPR Gap Analysis Report

Prepared for : [COMPANY NAME]

By: Compliance Partners

Date: [REPORT DATE]



www.compliancepartners.com



hello@compliancepartners.com



Table of Contents

Introduction	3
<hr/>	
Executive Summary	5
<hr/>	
Review & Analysis of Original Record of Processing Activities (RoPA)	6
<hr/>	
Introduction of new RoPA	8
<hr/>	
Data Protection Impact Assessments (DPIAs)	10
<hr/>	
Data Processing Agreements (DPAs)	11
<hr/>	
Third Country Impact Assessments (TIAs)	13
<hr/>	
Conclusion	14

Introduction

Compliance Partners recently completed a comprehensive GDPR Gap Analysis for your company to evaluate the organization's current compliance with the General Data Protection Regulation (GDPR).

As a result of this analysis, we have pinpointed areas where improvements are recommended or necessary to achieve the following goals:

- **Elevating the overall level of GDPR compliance within the organization**
- **Enhancing existing data protection practices**
- **Mitigating risks associated with data processing activities**

Our findings and recommendations are designed to guide you towards stronger data privacy and security practices.

Below you will find a description of the key terms we structure the gap analysis around; observations, recommendations and required actions.

We want to thank your team for their collaboration so far, and we look forward to continuing our partnership and supporting you in achieving effortless compliance.

Best regards,

The Effortless Compliance Team at Compliance Partners



Key Terms



Observation

These sections highlight findings or remarks noted during our assessment. They serve to inform you about certain aspects of your data processing practices. These observations don't require immediate action or changes from your side. Instead, they're meant to provide insights and raise awareness about specific areas without needing corrective measures.



Recommendation

The term "Recommendation" is used by Compliance Partners to describe suggested actions that you should consider taking based on our findings. Recommendations are aimed at enhancing compliance, improving data protection practices, and mitigating risks identified during the assessment.

While Compliance Partners can assist you in implementing these recommendations and provide tools and frameworks to decrease the workload and streamline internal processes, you play a key role in ensuring these tasks or actions are completed.



Required Action

The term "Required Action" is used by Compliance Partners to describe tasks that will be undertaken by Compliance Partners. However, these tasks will require collaboration and input from you, as well as your approval, to ensure successful completion. While Compliance Partners will drive the process, your involvement is essential for the execution and finalization of these actions.



Executive Summary

The GDPR Gap Analysis revealed several key findings regarding your company's data management practices:

1. Data Collection and Consent

The analysis identified that your company's data collection practices are largely compliant with GDPR requirements. However, there were several areas where consent was not properly documented or where the scope of data collection was unclear.

2. Data Storage and Security

Your company's data storage practices are generally sound, but the analysis revealed that certain data sets are not adequately secured. Specifically, there were concerns about the use of unencrypted email for transmitting sensitive data and the lack of access controls for certain internal systems.

3. Data Processing and Sharing

The analysis found that your company's data processing and sharing practices are mostly compliant. However, there were instances where data was shared with third parties without proper documentation or where the purpose of processing was not clearly defined.

4. Data Retention and Deletion

Your company's data retention and deletion practices are generally compliant. However, the analysis revealed that certain data sets are retained for longer than necessary, and there is a lack of a formal process for deleting data when it is no longer needed.

5. Data Breach Response

The analysis found that your company's data breach response plan is well-developed and includes clear roles and responsibilities. However, there were some gaps in the plan, particularly regarding the notification of affected individuals and the documentation of the response process.

6. Overall Findings

The analysis concluded that your company's data management practices are generally compliant with GDPR requirements. However, there were several areas where improvements were needed, particularly in the areas of consent, data security, and data retention.

1. Review & Analysis of Original Record of Processing Activities (RoPA)

Compliance Partners conducted an extensive review of your company's Register of Processing Activities (RoPA) as part of the onboarding procedure. Our objectives were to determine:

1. Whether the current state of the RoPA complies with the regulatory requirements outlined in Article 30 of the GDPR,
2. The accuracy of the information contained within the RoPA.

To achieve these objectives, we performed thorough business unit interviews across the organization. This in-depth approach allowed us to gather comprehensive insights into their data processing activities. We meticulously analyzed the existing RoPA, cross-referencing it with the information obtained from the interviews to ensure a detailed and accurate comparison.

On the next page are the documented observations from our analysis of the original RoPA and the actions steps we recommend:





Observation

Under the category Evaluation & Testing, our analysis and business plan interviews have identified an important role within the following criteria to which appears to be in place:

A)

Observation and evaluation of the business plan
The business plan is a document that outlines the business's goals, objectives, and strategies. It is a key tool for management to understand the business's current state and to plan for the future. The business plan should be updated regularly to reflect changes in the business environment and to ensure that the business is on track to achieve its goals.

B)

Business plan implementation and monitoring
The business plan is not just a document, but a living document that should be used to guide the business's operations. It should be implemented and monitored regularly to ensure that the business is on track to achieve its goals. The business plan should be updated regularly to reflect changes in the business environment and to ensure that the business is on track to achieve its goals.





2. Introduction of New Record of Processing Activities (RoPA)

We are pleased to introduce a newly developed Record of Processing Activities (RoPA) for your company. This comprehensive RoPA is the result of an in-depth analysis of your company's data processing activities, ensuring it aligns perfectly with the specific needs and operations of your organization.

Our primary objective in creating this new RoPA was to gain a thorough understanding of how personal data is processed within your company. By closely examining each step of data collection, storage, sharing, and retention, we aimed to develop a RoPA that provides clear insights into the lifecycle of personal data across various systems and processes.

Key advantages of having a RoPA in place:

- 1. Enhanced Regulatory Compliance:** Ensures adherence to GDPR and other relevant data protection regulations by documenting how personal data is processed within the organization.
- 2. Improved Data Management:** Provides a clear overview of data flows and dependencies, facilitating efficient data management practices, including data minimization and accurate data classification.
- 3. Risk Mitigation:** Identifies potential data privacy risks and areas of non-compliance, allowing for proactive measures to prevent data breaches and unauthorized access.
- 4. Support for Business Processes:** Aligns data processing activities with business logic and workflows, making it easier to implement security measures and maintain coherence with organizational processes.

Enhanced Transparency and Accountability:

Demonstrates a commitment to data protection and transparency to stakeholders, including customers, regulators, and business partners, fostering trust and accountability within the organization.



Required Action



100%

20% Effort and 100% Compliant

80%

Annual Compliance Wheel

60%

Ongoing GDPR Activities

40%

Onboarding and initial health check

20%

GDPR Scanner of shared drives, emails etc

3. DPIA, GDPR Article 35 (Data Protection Impact Assessment) Evaluation and Implementation for GDPR Compliance

As part of our GDPR review, Compliance Partners has conducted a thorough analysis of the processing activities within your company. One critical aspect of this assessment involves the identification and implementation of Data Protection Impact Assessments (DPIAs) as required under Article 35 of the General Data Protection Regulation (GDPR). DPIAs are essential tools for assessing and mitigating risks associated with data processing activities, ensuring compliance with GDPR principles and safeguarding individuals' rights to privacy and data protection.

A Data Protection Impact Assessment (DPIA) is a process designed to help organizations identify and minimize the data protection risks of processing activities. Under GDPR, DPIAs are required for processing activities that are likely to result in a high risk to the rights and freedoms of individuals.

As a general rule, DPIA's are needed in the following situations:

- When a new data processing activity is introduced that is likely to result in a high risk to individuals' rights and freedoms
- When significant changes are made to existing data processing activities that may impact the risk profile
- When processing involves systematic and extensive evaluation of personal aspects based on automated processing, including profiling
- When processing sensitive data or data on a large scale
- When monitoring publicly accessible areas on a large scale



Observation

The current data processing activities identified in the review are as follows:

- 1. Data collection
- 2. Data storage
- 3. Data processing
- 4. Data sharing
- 5. Data retention
- 6. Data deletion

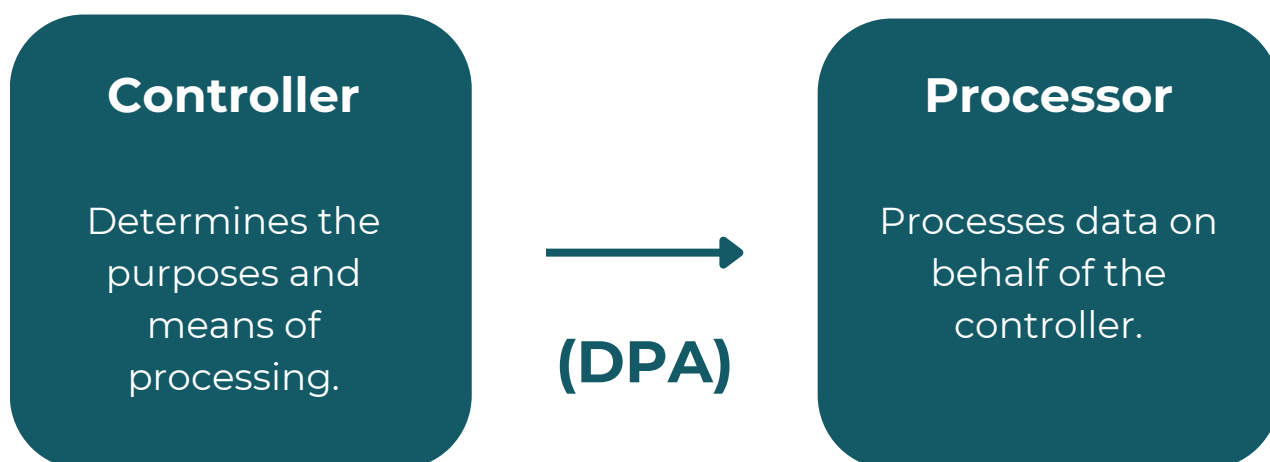
It is recommended that the organization implement the following measures to ensure compliance with GDPR:

- 1. Implement a data protection policy
- 2. Conduct a data protection impact assessment
- 3. Implement a data protection officer
- 4. Implement a data protection training program
- 5. Implement a data protection audit

4. DPA, GDPR Article 28, Section 3 (Data Processing Agreement) Evaluation and implementation for GDPR Compliance

In our ongoing efforts to ensure compliance with the General Data Protection Regulation (GDPR), Compliance Partners has conducted a thorough examination of your company data processing practices. A crucial aspect of this assessment involves the identification and evaluation of Data Processing Agreements (DPAs), which are essential contractual instruments for governing relationships with data processors as required by Article 28 of the GDPR.

Data Processing Agreements (DPAs) are critical components in GDPR compliance, particularly in managing relationships with third-party data processors. Article 28 of the GDPR mandates that whenever a controller uses a processor to process personal data on its behalf, there must be a written agreement in place (DPA). This agreement ensures that both parties understand their obligations and responsibilities under GDPR.





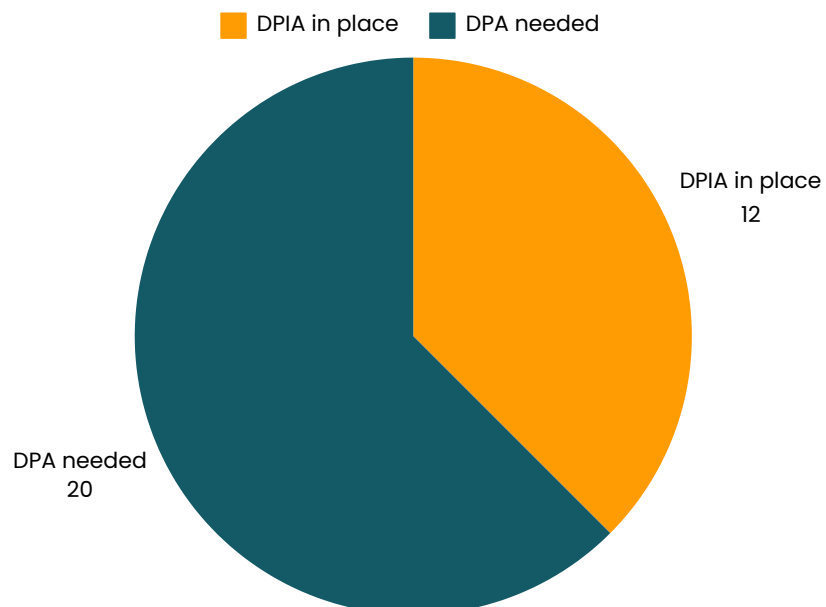
Observation

Observation is a research method that involves watching and recording behavior in its natural setting. It is often used to study social interactions, group dynamics, and individual actions. The researcher typically does not intervene or manipulate the environment, but rather observes and records what is happening naturally.

There are several types of observation, including participant observation (where the researcher is part of the group being studied) and non-participant observation (where the researcher is an outsider). Observation can be structured (with predefined categories and codes) or unstructured (more open-ended and flexible).

Observation is a valuable method for understanding human behavior and social interactions. It provides rich, detailed data that can be used to develop theories and inform practice. However, it can be time-consuming and may be subject to biases, such as observer effects or selective reporting.

- Participant observation
- Non-participant observation
- Structured observation
- Unstructured observation
- Direct observation
- Indirect observation
- Covert observation
- Overt observation
- Naturalistic observation
- Laboratory observation



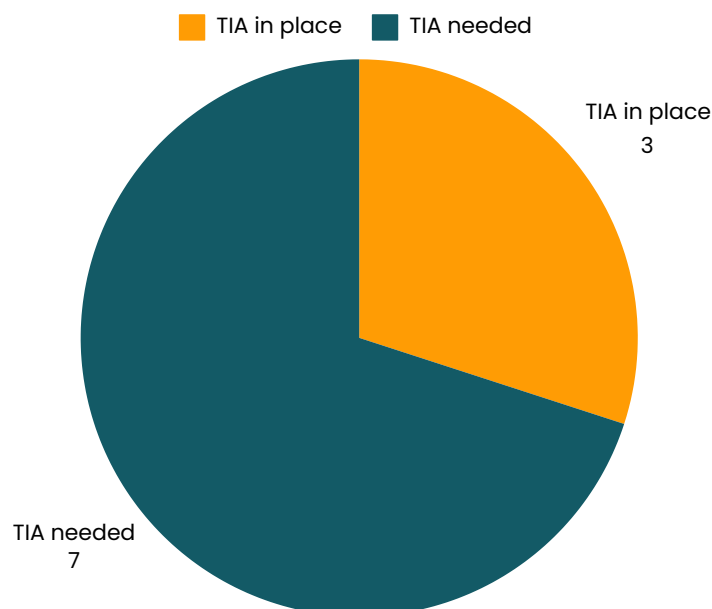
5. TIA, GDPR Article 46.2 and 46.3 (Transfer Impact Assessment) Evaluation and Implementation for GDPR Compliance

Transfer Impact Assessments (TIAs) are evaluations conducted by data controllers and processors to assess the level of protection afforded to personal data when it is transferred internationally. The primary aim is to ensure that the transferred data receives an equivalent level of protection as it would under GDPR regulations.

TIAs are required whenever personal data is transferred to a country outside the EEA that does not benefit from an adequacy decision by the European Commission.

Compliance Partners has conducted a review of your company's data processing activities, particularly focusing on international data transfers.

As a result, the graph below illustrates the identified Transfer Impact Assessments in place and those that are instead missing.



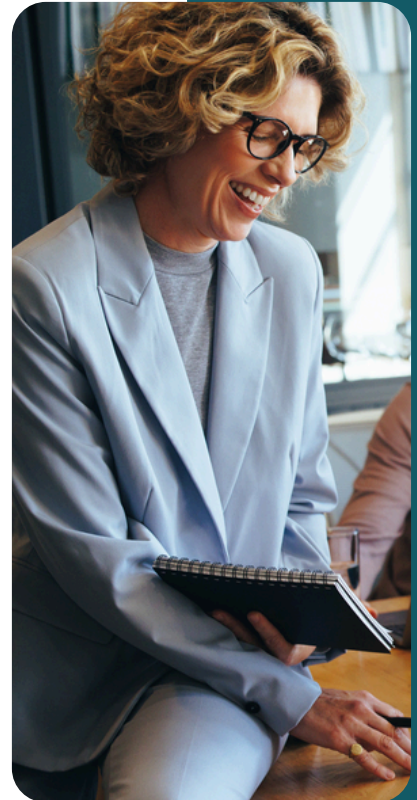
Conclusion

The findings of this analysis indicate that the organization has made significant progress in addressing the identified gaps. The implementation of the recommended controls has resulted in a more robust and effective compliance program. The organization's commitment to transparency and ethical conduct is evident in the thoroughness of the review and the proactive measures taken to address the findings. The continued monitoring and evaluation of the program will ensure its ongoing effectiveness and alignment with the organization's values and mission.

The organization's leadership has demonstrated a strong commitment to the integrity of the compliance program. The clear communication of the findings and the implementation of the recommended controls have fostered a culture of accountability and continuous improvement. The organization's dedication to the highest standards of ethical conduct is a testament to its commitment to excellence and its commitment to the well-being of its stakeholders.

The organization's commitment to transparency and ethical conduct is evident in the thoroughness of the review and the proactive measures taken to address the findings. The continued monitoring and evaluation of the program will ensure its ongoing effectiveness and alignment with the organization's values and mission. The organization's leadership has demonstrated a strong commitment to the integrity of the compliance program. The clear communication of the findings and the implementation of the recommended controls have fostered a culture of accountability and continuous improvement.

The organization's dedication to the highest standards of ethical conduct is a testament to its commitment to excellence and its commitment to the well-being of its stakeholders. The continued monitoring and evaluation of the program will ensure its ongoing effectiveness and alignment with the organization's values and mission. The organization's leadership has demonstrated a strong commitment to the integrity of the compliance program. The clear communication of the findings and the implementation of the recommended controls have fostered a culture of accountability and continuous improvement.



Curious About Your GDPR Gaps?

Our Effortless Compliance Team is here to provide a comprehensive gap report and guide you through the necessary steps to achieve full compliance effortlessly.

Contact Us to
Know More

www.compliancepartners.com
hello@compliancepartners.com

Get Local Support

Denmark

+45 89 87 11 15

Sweden

+46 10 888 52 76

Finland

+358 75 3251388

Germany

+49 32 221855955