TOPCERTIFIER

Governance, Risk & Compliance Consultants

GDPR GAP ANALYSIS TEMPLATE

INTRODUCTION:

TopCertifier offers a Simplified GDPR Compliance Gap Analysis Checklist to help you identify areas where your organization may need improvements to align with GDPR regulations. This checklist serves as an initial step in assessing your GDPR compliance.

SECTION 1: DATA MAPPING AND PROCESSING

- ☐ Have you identified all types of personal data collected and processed?
- ☐ Is it clear why and how each type of personal data is being processed?
- ☐ Do you have a record of the legal basis for processing personal data for each processing activity?

SECTION 2: CONSENT AND DATA SUBJECT RIGHTS

- ☐ Do you obtain explicit consent for data processing where required?
- ☐ Is there a process to respond to requests for access, rectification, and data portability?
- ☐ Are procedures in place to ensure the rights of minors and for consent?

SECTION 3: PRIVACY POLICIES AND COMMUNICATION

- ☐ Do you have clear and comprehensive privacy policies that align with requirements?
- ☐ Is there a mechanism to communicate your privacy policies to data subjects?
- ☐ Are the privacy policies easily accessible and written in clear and plain language?

SECTION 4: DATA SECURITY AND BREACH RESPONSE

- ☐ Have you implemented appropriate security measures to safeguard personal data?
- ☐ Is there a documented process to detect, report, and investigate data breaches?
- ☐ Are your employees adequately trained on data security procedures?

SECTION 5: DATA TRANSFER AND THIRD-PARTIES

- ☐ Do you ensure that international data transfers comply with GDPR regulations?
- ☐ Is there a due diligence process to assess third-party compliance before sharing data?
- ☐ Are contracts with third parties processing data on your behalf GDPR-compliant?

SECTION 6: DATA PROTECTION IMPACT ASSESSMENTS

- ☐ Are DPIAs conducted for high-risk processing activities?
- ☐ Do the DPIAs include an assessment of necessity, and risk mitigation measures?
- ☐ Are DPIAs periodically reviewed and updated as necessary?

SECTION 7: DPO AND ACCOUNTABILITY

- ☐ Have you appointed a Data Protection Officer (DPO) if required by GDPR?
- ☐ Is the DPO adequately involved in all issues related to the protection of personal data?
- ☐ Is there a system of accountability and governance to demonstrate compliance with GDPR?

Please note that this checklist provides a high-level overview. It is important to perform a thorough analysis specific to your organization's processes and context. Additionally, engaging with GDPR experts or consultants to conduct a comprehensive gap analysis is recommended.