Data Storage, Personal Data Security, and Communication Permissions Policy in Compliance with Turkish Personal Data Protection Law (Law No. 6698) Introduction: • Brief explanation emphasizing the importance of secure data storage, personal data protection, and communication permissions in compliance with Turkish regulations, specifically the Turkish Personal Data Protection Law (KVKK - Law No. 6698). Section 1: Overview of Turkish Personal Data Protection Law (KVKK - Law No. 6698): • Concise explanation of the relevant sections within KVKK that specifically pertain to data storage, personal data security, and communication permissions. • Highlighting the legal requirements and obligations outlined in KVKK concerning these areas. Section 2: Principles of Secure Data Storage and Personal Data Protection under KVKK (Law No. 6698): • Elaboration on the key principles mandated by KVKK concerning secure data storage and personal data protection, including integrity, confidentiality, and accountability. • Emphasis on the importance of implementing these principles within the organization's data storage practices. Section 3: Data Storage Procedures and Compliance with KVKK (Law No. 6698): • Detailed guidelines for secure data storage practices in compliance with KVKK requirements. • Specific procedures for encryption, access controls, backups, and data retention periods as required by the law. Section 4: Personal Data Security Measures in Compliance with KVKK (Law No. 6698): • Elaboration on the technical and organizational measures to ensure personal data security in accordance with KVKK. • Description of access controls, encryption methods, regular security assessments, and measures to prevent unauthorized access or breaches. Section 5: Communication Permissions and Data Handling: • Guidelines and procedures for obtaining explicit communication permissions from individuals before data processing, in compliance with KVKK requirements. • Specific details on documenting and managing communication permissions within the organization's data handling processes. Section 6: Data Breach Response and Notification Procedures: • Detailed procedures for handling data breaches in line with KVKK requirements, including immediate response, investigation, and notification protocols. • Explanation of reporting obligations and timeframes for data breach notifications as per KVKK stipulations. Section 7: Training and Awareness on Secure Data Handling: • Description of ongoing training programs to educate employees about secure data handling practices mandated by KVKK. • Emphasis on regular training sessions to ensure compliance and understanding of data protection obligations. Section 8: Compliance Monitoring and Updates: • Measures for regular audits, assessments, and monitoring mechanisms to ensure compliance with the Data Storage, Personal Data Security, and Communication Permissions Policy and KVKK regulations. • Protocols for reviewing and updating the policy in line with legislative changes mandated by KVKK. Conclusion: • Recapitulation of the crucial role of secure data storage, personal data security, and communication permissions in compliance with Turkish Personal Data Protection Law (KVKK - Law No. 6698). • Emphasis on the commitment to implementing robust data storage practices, safeguarding personal data, and obtaining proper communication permissions as per KVKK requirements.