KSA PDPL Compliance Checklist for F&B Companies

PDPL Compliance Table for Multi-Channel F&B Operations (Dine-in, Delivery, Subscription)

Specifically tailored for food & beverage businesses handling customer data including: dietary preferences, delivery addresses, payment information, loyalty programs, subscription meal plans, and health-related food requirements.

Requirement	PDPL Article	Compliance Check	Red Flags	Risk (Likelihood/Impact)	Consequences of Breach
GOVERNANCE & ACCOUNTABILITY					
Data Protection Officer	Art. 32	Appointed a qualified Data Protection Officer	• No dedicated DPO • DPO lacks necessary qualifications • DPO has conflicts of interest	Medium/High	• Fines up to SAR 5 million • Regulatory investigation • Inability to demonstrate compliance
	Art. 32, 33	Defined DPO responsibilities and authority	• Unclear reporting structure • Insufficient authority • No documented responsibilities	Medium/Medium	• Fines up to SAR 3 million • Ineffective compliance program
	Art. 32, 33	Established direct reporting line to executive management	• DPO reports to mid-level management • No access to board/executives	Low/Medium	• Regulatory criticism • Operational inefficiencies
Data Protection Strategy	Art. 4, 14	Developed comprehensive data protection policy	• Generic policies not tailored to F&B operations • Outdated policies • No documentation	High/High	• Fines up to SAR 5 million • Systematic non-compliance • Reputational damage

KSA PDPL Compliance Checklist for F&B Companies

PDPL Compliance Table for Multi-Channel F&B Operations (Dine-in, Delivery, Subscription)

Requirement	PDPL Article	Compliance Check	Red Flags	Risk (Likelihood/Impact)	Consequences of Breach
	Art. 12	Created channel-specific data handling procedures	• Same procedures across all channels • Ignoring unique risks of delivery/subscription	Medium/High	• Data leaks • Customer complaints • Regulatory scrutiny
Internal Compliance	Art. 30, 31	Established data protection audit schedule	• No regular audits • Audit findings not addressed • Self-assessment only	Medium/Medium	• Undetected compliance gaps • Prolonged non-compliance
LAWFUL PROCESSING & CONSENT					
Lawful Basis	Art. 5, 6	Identified lawful basis for each processing activity	• Relying on consent when another basis applies • Processing without valid basis • No documentation of basis	High/High	• Fines up to SAR 3 million • Processing prohibition • Customer complaints
Consent Management	Art. 10, 11	Designed clear consent mechanisms at all touchpoints	• Pre-ticked boxes • Bundled consent • No evidence of consent	High/High	• Illegal data processing • Fines up to SAR 3 million • Requirement to delete data
	Art. 11	Implemented age verification for consent	• No age verification	Medium/High	• Severe penalties (up to SAR 3 million)

KSA PDPL Compliance Checklist for F&B Companies

PDPL Compliance Table for Multi-Channel F&B Operations (Dine-in, Delivery, Subscription)

Requirement	PDPL Article	Compliance Check	Red Flags	Risk (Likelihood/Impact)	Consequences of Breach
			• Processing children's data without parental consent		• Processing prohibition
	Art. 10	Established process for consent withdrawal	• Difficult withdrawal process for loyalty programs • No way to opt out of marketing communications • Continued processing after consent withdrawal	High/Medium	• Fines • Customer complaints • Regulatory investigation
Notification	Art. 14	Created comprehensive privacy notices	• Missing required elements • Overly complex language • Notices not easily accessible	High/Medium	• Fines up to SAR 3 million • Transparency violations
DATA COLLECTION & PROCESSING					
Restaurant Operations	Art. 6, 8	Implemented data minimization for reservation systems	• Collecting excessive data beyond booking needs (e.g., unnecessary dietary info) • Keeping all historical reservations indefinitely	High/Medium	• Fines • Data deletion orders • Customer trust erosion

KSA PDPL Compliance Checklist for F&B Companies

PDPL Compliance Table for Multi-Channel F&B Operations (Dine-in, Delivery, Subscription)

Requirement	PDPL Article	Compliance Check	Red Flags	Risk (Likelihood/Impact)	Consequences of Breach
			• Recording customer preferences without purpose		
	Art. 6, 8	Established secure handling of payment information	• Unencrypted payment data • Excessive retention of payment details • Unnecessary storage of CVV	High/High	• Payment fraud • Severe fines • Legal liability for data breach
Delivery Operations	Art. 6, 8	Established secure handling of customer location data	• Tracking customer location beyond delivery window • Retaining precise delivery locations after order completion • Using location data for targeted promotions without consent	Medium/High	• Location data breach • Customer privacy violations • Regulatory penalties
	Art. 6, 8	Implemented data minimization for delivery addresses	• Keeping all historical addresses • Sharing addresses with marketing partners	Medium/Medium	• Fines • Customer complaints
Subscription Service	Art. 5, 25	Implemented secure handling of dietary preferences	• Not recognizing allergy information as sensitive health data • Using customer meal preferences for	Medium/High	• Processing prohibition • Severe penalties (health data)

KSA PDPL Compliance Checklist for F&B Companies

PDPL Compliance Table for Multi-Channel F&B Operations (Dine-in, Delivery, Subscription)

Requirement	PDPL Article	Compliance Check	Red Flags	Risk (Likelihood/Impact)	Consequences of Breach
			marketing without consent • Sharing nutritional plans with third parties		• Regulatory enforcement
	Art. 9	Established protocols for subscription payment information	• Storing complete payment details • Insecure payment storage • No tokenization	High/High	• Payment data breach • Fines • Legal action
Special Categories	Art. 5	Identified all health-related data collected	• Not recognizing food allergies as health data • Treating weight management meal plans as regular data • No special protection for halal/kosher requirements	High/High	• Severe penalties (up to SAR 3 million) • Processing prohibition • Required deletion of improperly collected data
DATA SUBJECT RIGHTS					
Access Rights	Art. 15, 16	Established procedure for handling data access requests	• No formal DSAR process • Excessive response times • Incomplete data provision	Medium/High	• Fines up to SAR 3 million • Regulatory enforcement • Loss of customer trust
	Art. 16	Created user-friendly	• Complex request procedures	Medium/Medium	• Regulatory criticism

KSA PDPL Compliance Checklist for F&B Companies

PDPL Compliance Table for Multi-Channel F&B Operations (Dine-in, Delivery, Subscription)

Requirement	PDPL Article	Compliance Check	Red Flags	Risk (Likelihood/Impact)	Consequences of Breach
		mechanisms for access requests	• Multiple steps to request data • No digital request option		• Customer frustration
Rectification Rights	Art. 18	Implemented procedures for correcting inaccurate data	• No correction mechanism • Delays in making corrections • Corrections not propagated to all systems	Medium/Medium	• Fines • Incorrect decisions based on wrong data
	Art. 19	Created processes for erasure requests	• No "right to be forgotten" mechanism • Incomplete deletion • No verification of deletion requests	High/Medium	• Fines up to SAR 3 million • Continued data protection obligations
Additional Rights	Art. 20	Established procedures for data portability	• No data export capability • Non-machine-readable formats • Incomplete data portability	Low/Medium	• Regulatory criticism • Fines
DATA SECURITY					
Technical Security	Art. 34, 35	Implemented encryption for data at rest and in transit	• Unencrypted customer databases • Plain text customer communications	High/High	• Data breaches • Severe penalties

KSA PDPL Compliance Checklist for F&B Companies

PDPL Compliance Table for Multi-Channel F&B Operations (Dine-in, Delivery, Subscription)

Requirement	PDPL Article	Compliance Check	Red Flags	Risk (Likelihood/Impact)	Consequences of Breach
			• No encryption standards		• Mandatory breach notification
	Art. 39, 40	Established access controls based on need-to-know	• Excessive access rights • Shared login credentials • No access reviews	High/High	• Insider threats • Unauthorized access • Data leakage
POS Security	Art. 39, 40	Established PCI-DSS compliance for payment processing	• Non-compliant POS systems • Outdated software/hardware • Payment data exposure	High/High	• Payment fraud • PCI fines • PDPL penalties
	Art. 39, 40	Implemented secure handling of receipt data	• Full card numbers on receipts • Excessive customer details on receipts	Medium/Medium	• Identity theft risk • Customer complaints
Mobile App Security	Art. 34, 35	Implemented secure authentication for customer accounts	• Weak password requirements in food ordering app • Auto-saved payment details without additional verification • Persistent login without session timeouts	High/High	• Unauthorized food orders • Payment fraud • Exposure of delivery addresses

KSA PDPL Compliance Checklist for F&B Companies

PDPL Compliance Table for Multi-Channel F&B Operations (Dine-in, Delivery, Subscription)

Requirement	PDPL Article	Compliance Check	Red Flags	Risk (Likelihood/Impact)	Consequences of Breach
Physical Security	Art. 39, 40	Implemented secure storage of physical records	• Customer forms left visible • Unsecured storage areas • Improper disposal	Medium/Medium	• Physical data theft • Regulatory fines • Customer privacy violations
THIRD PARTY MANAGEMENT					
Delivery Partners	Art. 23, 24	Established data processing agreements	• No formal agreements with third-party delivery services • No restrictions on delivery personnel access to customer data • No provisions for deleting customer addresses after delivery	High/High	• Unauthorized data processing • Liability for delivery partner data misuse • Fines up to SAR 3 million
	Art. 23, 24	Created data transfer protocols for sharing only necessary data	• Sharing complete customer profiles with delivery drivers • Sending unnecessary personal data to payment processors • No data minimization in third-party integrations	Medium/High	• Data leaks • Unauthorized use • Regulatory penalties

KSA PDPL Compliance Checklist for F&B Companies

PDPL Compliance Table for Multi-Channel F&B Operations (Dine-in, Delivery, Subscription)

Requirement	PDPL Article	Compliance Check	Red Flags	Risk (Likelihood/Impact)	Consequences of Breach
Payment Processors	Art. 23, 24	Implemented data processing agreements	• No formal agreements • No security requirements • No audit rights	High/High	• Payment data breaches • Joint liability • Regulatory fines
Cloud Providers	Art. 23, 24, 29	Established data processing agreements with cloud providers	• No cloud agreements • Missing required clauses • No security assurances	High/High	• Unauthorized processing • Cross-border transfer violations • Severe penalties
Marketing Partners	Art. 23, 24	Established data sharing limitations	• Unrestricted data sharing • No purpose limitation • No oversight of usage	Medium/High	• Unauthorized marketing • Customer complaints • Fines
CROSS-BORDER TRANSFERS					
Transfer Framework	Art. 28, 29	Identified all cross-border data transfers	• Unidentified transfers • No transfer mapping • Hidden transfers (cloud, analytics)	High/High	• Illegal transfers • Severe penalties (up to SAR 3 million) • Transfer prohibition
	Art. 28, 29	Obtained SDAIA approval where required	• Transfers without approval	High/High	• Transfer prohibition

KSA PDPL Compliance Checklist for F&B Companies

PDPL Compliance Table for Multi-Channel F&B Operations (Dine-in, Delivery, Subscription)

Requirement	PDPL Article	Compliance Check	Red Flags	Risk (Likelihood/Impact)	Consequences of Breach
			• No documentation of approvals • Transfers to unauthorized countries		• Severe penalties • Operational disruption
Cloud Compliance	Art. 28, 29	Verified data residency options	• Restaurant management systems hosted on non-compliant cloud servers • Online ordering data stored outside KSA without proper safeguards • Customer databases on international servers without transfer mechanisms	High/High	• Illegal transfers • Service disruption • Severe penalties
DATA BREACH MANAGEMENT					
Detection & Response	Art. 36, 37	Implemented breach detection technologies	• No monitoring systems • Delayed detection capabilities • Inadequate logging	High/High	• Undetected breaches • Extended impact • Notification failures
Detection & Response	Art. 36, 37	Established incident response team	• No designated response team for	Medium/High	• Delayed breach containment

KSA PDPL Compliance Checklist for F&B Companies

PDPL Compliance Table for Multi-Channel F&B Operations (Dine-in, Delivery, Subscription)

Requirement	PDPL Article	Compliance Check	Red Flags	Risk (Likelihood/Impact)	Consequences of Breach
			restaurant data breaches • Untrained staff handling incident response • No escalation procedures for data incidents		• Extended breach impact • Regulatory scrutiny
Notification	Art. 36, 37	Created process for notifying SDAIA within 72 hours	• No notification procedures • Missed notification deadlines • Incomplete notifications	High/High	• Additional penalties • Regulatory investigation • Loss of trust
Notification	Art. 36, 37	Established criteria for notifying affected individuals	• No procedure for notifying customers of compromised payment data • No templates for breach communications • Inadequate notification content	Medium/High	• Reputation damage • Customer legal action • Regulatory penalties
DATA LIFECYCLE MANAGEMENT					
Data Collection	Art. 6, 8	Implemented data	• Excessive data fields • Collection without purpose	High/Medium	• Unnecessary data liability

KSA PDPL Compliance Checklist for F&B Companies

PDPL Compliance Table for Multi-Channel F&B Operations (Dine-in, Delivery, Subscription)

Requirement	PDPL Article	Compliance Check	Red Flags	Risk (Likelihood/Impact)	Consequences of Breach
		minimization at collection	• Default collection of optional data		• Regulatory criticism • Data deletion requirements
Retention & Disposal	Art. 12	Established retention periods for each data category	• Indefinite retention • No retention policy • One-size-fits-all retention	High/Medium	• Data hoarding • Illegal retention • Increased breach impact
	Art. 12	Created automated deletion workflows	• Manual deletion only • No deletion verification • Incomplete deletion	Medium/Medium	• Retention violations • Continued data liability • Regulatory penalties
OPERATIONAL INTEGRATION					
Reservation Systems	Art. 5, 6, 8	Implemented data protection in reservation workflows	• Excessive data collection • No privacy notices • Secondary use without consent	Medium/Medium	• Unlawful processing • Regulatory penalties • Customer complaints
Loyalty Programs	Art. 5, 6, 8	Established lawful basis for loyalty program data	• Auto-enrolling customers without explicit consent • Using order history to create detailed customer profiles	High/Medium	• Unlawful processing • Fines • Forced program changes

KSA PDPL Compliance Checklist for F&B Companies

PDPL Compliance Table for Multi-Channel F&B Operations (Dine-in, Delivery, Subscription)

Requirement	PDPL Article	Compliance Check	Red Flags	Risk (Likelihood/Impact)	Consequences of Breach
			• Mining dining patterns for secondary marketing purposes		
	Art. 10, 11	Created transparency notices for loyalty programs	• Hidden terms • Unclear data usage explanation • Missing information on data sharing	Medium/Medium	• Transparency violations • Customer distrust • Regulatory criticism
Customer Feedback	Art. 5, 6, 8	Implemented anonymization options for feedback	• Requiring personally identifiable information for all feedback • No option for anonymous reviews/comments • Storing feedback with identifiers indefinitely	Low/Medium	• Excessive data risk • Customer reluctance to provide feedback • Unnecessary data liability
Nutritional Planning	Art. 5	Established enhanced security for dietary/health data	• Storing calorie-controlled meal plan data insecurely • Not isolating medical diet information (diabetes, heart disease) • Allowing staff without need-to-know to access health-related meal restrictions	High/High	• Severe penalties (health data) • Processing prohibition • Customer health impacts from inappropriate disclosure

KSA PDPL Compliance Checklist for F&B Companies

PDPL Compliance Table for Multi-Channel F&B Operations (Dine-in, Delivery, Subscription)

Requirement	PDPL Article	Compliance Check	Red Flags	Risk (Likelihood/Impact)	Consequences of Breach
EMPLOYEE TRAINING					
Training Program	Art. 32, 33	Developed role-specific data protection training	• Same training for all F&B staff regardless of role • No specific guidance for waitstaff handling customer data • No training on handling visible dietary restriction notes	Medium/Medium	• Front-of-house staff mishandling sensitive data • Customer complaints about privacy • Preventable data exposure incidents
	Art. 39	Established mandatory training frequency	• One-time training only • No refresher courses • No training verification	Medium/Medium	• Knowledge gaps • Outdated practices • Compliance deterioration
Awareness Activities	Art. 32, 33	Created data protection guidelines for daily operations	• No practical guidance for servers on handling payment cards • No protocols for taking down customer information • No visual reminders about data protection in staff areas	Medium/Medium	• Day-to-day violations • Inconsistent data handling practices • Preventable privacy incidents
DOCUMENTATION & EVIDENCE					

KSA PDPL Compliance Checklist for F&B Companies

PDPL Compliance Table for Multi-Channel F&B Operations (Dine-in, Delivery, Subscription)

Requirement	PDPL Article	Compliance Check	Red Flags	Risk (Likelihood/Impact)	Consequences of Breach
Processing Records	Art. 12, 39	Created records of processing activities	• Incomplete records • Outdated information • Missing processing purposes	High/Medium	• Inability to demonstrate compliance • Regulatory penalties • Failed audits
	Art. 12, 39	Developed documentation of lawful bases	• Missing documentation • Generic justifications • No specific legal basis cited	High/Medium	• Unlawful processing findings • Regulatory challenges • Fines
Compliance Evidence	Art. 37, 39	Established documentation of policies and procedures	• Missing documentation • Outdated policies • Generic non-tailored documents	Medium/Medium	• Inability to demonstrate compliance • Failed audits • Regulatory scrutiny
TECHNOLOGY SYSTEMS					
POS Systems	Art. 34, 35	Conducted PDPL compliance assessment	• Restaurant POS systems displaying full credit card details • Customer profile data visible on cashier screens	High/High	• Customer data visible to all restaurant staff • Payment data breaches • Regulatory penalties

KSA PDPL Compliance Checklist for F&B Companies

PDPL Compliance Table for Multi-Channel F&B Operations (Dine-in, Delivery, Subscription)

Requirement	PDPL Article	Compliance Check	Red Flags	Risk (Likelihood/Impact)	Consequences of Breach
			• Storing customer order history indefinitely in POS		
CRM Systems	Art. 39, 40	Implemented access controls based on necessity	• Excessive user access • No access reviews • Shared credentials	High/High	• Customer data leakage • Insider threats • Unauthorized access
Mobile Applications	Art. 39, 40	Conducted PDPL assessment of mobile apps	• Excessive app permissions • Background data collection • Third-party SDKs with data access	High/High	• Mobile data breaches • Customer privacy violations • Regulatory investigation
	Art. 14	Established transparent privacy notices within apps	• Hidden privacy information in food ordering app • Unclear explanation of how customer preferences are used • No in-app privacy controls for users	Medium/Medium	• Transparency violations • Customer complaints • Forced app changes
ONGOING COMPLIANCE					
Monitoring	Art. 30, 31	Established KPIs for data protection compliance	• No metrics for measuring restaurant compliance	Medium/Medium	• Undetected compliance issues

KSA PDPL Compliance Checklist for F&B Companies

PDPL Compliance Table for Multi-Channel F&B Operations (Dine-in, Delivery, Subscription)

Requirement	PDPL Article	Compliance Check	Red Flags	Risk (Likelihood/Impact)	Consequences of Breach
			• No regular reporting on data protection • No tracking of access to customer databases		• No visibility into risk areas • Reactive rather than proactive approach
Regulatory Engagement	Art. 30, 31	Established procedures for regulatory inquiries	• No designated contact for SDAIA inquiries • Unprepared for regulatory questions about customer data • No documentation of data practices readily available	Medium/High	• Poor regulatory relations • Extended investigations • Higher penalties