DPDP ACT 2023+ CYBERSECURITY MAPPING CUSTOM GPT CHEAT SHEET

THIS GUIDE SHOWS HOW TO USE THE CUSTOM GPT ON DPDP ACT. HOW DPDP OBLIGATIONS ALIGN WITH MODERN SECURITY TOOLS LIKE SIEM, SOC, UEBA, ITDR, AND SOAR TO HELP ORGANISATIONS PROTECT PERSONAL DATA, DETECT THREATS FASTER, AND STAY SECURE IN AN EVOLVING DIGITAL LANDSCAPE.

PRESENTED BY :   **OMKAR NATH NANDI**

CUSTOM GPT, DPDP ACT GUIDE & SOLUTIONS
BIT.LY/3K4HN9M

DPDP ACT CUSTOM GPT & CYCBERSECURITY

FROM CONSENT TO CONTROLS

How consent and notices translate into real security checks.

THE DPDP SECURITY BRIDGE

How DPDP connects directly to your security stack and ops.

THE SECURITY SAFEGUARDS PLAYBOOK

A quick map of DPDP's safeguard duties to core security tools.

DPDP ESSENTIALS FOR SECURITY TEAMS

Key DPDP rules every SOC and security engineer must know.

DPDP RISK SIGNALS FOR SECURITY ANALYSTS

The alerts and anomalies that indicate potential DPDP violations.

DPDP ACT CUSTOM GPT & CYCBERSECURITY

DPDP-ALIGNED THREAT DETECTION USE CASES

Detection rules for SIEM and UEBA tied to DPDP obligations.

BREACH RESPONSE UNDER DPDP

What security teams must do when personal data is affected.ack and ops.

THE DPDP RETENTION & MINIMISATION MATRIX

How DPDP's retention rules link to data lifecycle controls.

IDENTITY IS THE NEW COMPLIANCE PERIMETER

How IAM and ITDR enforce DPDP rules by design.

DPDP COMPLIANCE IN THE SOC: A FIELD GUIDE

A quick framework to embed DPDP thinking into SOC workflows.

THE DPDP & CYBERSECURITY LINK MAP

DPDP compliance and cybersecurity are deeply connected: every consent, access request, and data flow creates signals security teams must protect. This cheat shows how personal data, purpose limitation, notice, and safeguard duties translate into logs, monitoring, detection, response, and internal controls required to stay compliant.

DPDP BASICS EVERY SOC MUST KNOW

Security teams must understand how DPDP defines personal data, consent, fiduciary responsibilities, storage limits, and breach obligations. This cheat highlights the core rules SOC analysts must recognise during triage, correlating alerts, handling investigations, and assessing whether an incident qualifies as a DPDP-related risk or breach requiring escalation.

LINKING CONSENT TO SECURITY TOOLS

Consent and notice requirements create a need for strong API monitoring, event logging, IAM controls, and secure app design. This cheat explains how security must ensure consent data is tamper-proof, logged correctly, protected from misuse, and monitored for abnormal changes to prevent unauthorized processing or hidden data extraction attempts.

SAFEGUARDS MAPPED TO SECOPS TOOLS

DPDP's "reasonable security safeguards" translate into continuous detection, identity hardening, encryption, and disciplined response. This cheat shows how SIEM, SOAR, UEBA, ITDR, XDR, and access controls work together to protect personal data, flag misuse, isolate threats, and ensure organisations can demonstrate compliance through verifiable security action trails.

DPDP RISK SIGNALS FOR ANALYSTS

Some alerts must immediately be treated as DPDP-relevant: abnormal DB queries, sudden exports, identity escalation, consent table changes, privileged misuse, or cross-border traffic anomalies. This cheat outlines how to identify these signals and elevate them for enhanced investigation, compliance reporting, and potential breach evaluation under DPDP requirements.

HANDLING BREACHES UNDER DPDP LAW

When personal data is at risk, teams must rapidly assess scope, confirm impact, preserve forensic logs, isolate compromised systems, and notify legal or leadership as required. This cheat maps every DPDP breach expectation to IR actions, evidence collection, SOAR playbooks, communication preparation, and documentation required for regulatory reporting.

IDENTITY AS THE CORE COMPLIANCE GATE

Identity systems control which users, apps, or services can access personal data. This cheat shows how IAM, PAM, MFA, and ITDR enforce purpose limitation, secure privileged access, detect compromised accounts, and prevent unauthorized data use. Strong identity posture becomes essential to proving compliant access and stopping insider or external misuse.

DPDP-ALIGNED SIEM USE CASE LIBRARY

Security teams must embed DPDP-specific detection rules: flag unusual access to personal data tables, monitor failed access attempts, detect mass downloads, identify unauthorized API calls, track consent DB edits, and correlate identity anomalies. This cheat provides a structured outline for building SIEM and UEBA use cases tied directly to DPDP obligations.

DATA RETENTION & MINIMISATION MATRIX

DPDP mandates retaining data only as long as needed and deleting or anonymising it thereafter. This cheat maps these mandates to retention rules, archival processes, automated cleanup jobs, backup rotation, and monitoring for outdated or shadow data stores. It ensures security teams help enforce lifecycle limits across systems storing personal information.

EMBEDDING DPDP INTO SOC WORKFLOW

Compliance must live inside daily SOC operations. This cheat explains how analysts can tag incidents as DPDP-related, structure investigations around personal data impact, use SOAR to automate escalation, log all evidence, and maintain auditable records. It ensures every alert touching personal data receives consistent, policy-aligned handling and documentation.

GENERAL DPDP INTERPRETATION PROMPTS

Explain Section 7 of the DPDP Act in simple language and give 3 real-world examples relevant to a SaaS company.

Summarise my obligations as a Data Fiduciary under DPDP in less than 10 points.

GENERAL DPDP INTERPRETATION PROMPTS

What are the DPDP compliance risks if an app collects user data without clear notice?

How does DPDP treat personal data vs sensitive personal data? Add examples.

MAPPING REAL SITUATIONS TO DPDP SECTIONS

Here is my business workflow. Map each step to the relevant DPDP sections and identify compliance gaps.

Is this workflow DPDP compliant? Identify issues and suggest corrections.

MAPPING REAL SITUATIONS TO DPDP SECTIONS

Does this scenario qualify as a DPDP breach? Explain step-by-step and list impacted sections.

Map our HR onboarding process to DPDP rules, and list improvements needed.

CYBERSECURITY + DPDP PROMPTS

A user downloaded 30K customer records at midnight. Map this incident to DPDP sections and identify SOC actions.

Create DPDP-compliant SIEM use cases for insider threats.

CYBERSECURITY + DPDP PROMPTS

Explain how SOAR workflows can support DPDP breach response.

Show how ITDR protects us from DPDP violations related to identity misuse.

CYBERSECURITY + DPDP PROMPTS

Our consent table had 500 records changed at once. Is this a DPDP risk? Explain.

Provide a DPDP-ready breach response playbook with detection, containment, and reporting steps.

DOCUMENTS, POLICIES & REVIEWS

Review this privacy policy and show all DPDP non-compliant parts. Provide corrected text. (Upload file.)

Generate a DPDP-compliant privacy notice for a mobile app.

DOCUMENTS, POLICIES & REVIEWS

Review our vendor contract and identify all DPDP gaps. Suggest clauses to fix them.

Create a DPDP-compliant data retention policy with timelines.

IMPLEMENTATION ROADMAPS

Create a 30-60-90 day DPDP implementation roadmap for a mid-size SaaS company.

Give me a DPDP technical controls checklist for engineering + security teams.

IMPLEMENTATION ROADMAPS

Summarise DPDP compliance tasks for HR, finance, marketing, IT, and security.

Give me a DPDP audit framework with checkpoints and evidence list.

IMPLEMENTATION ROADMAPS

Build a DPDP DPIA template for new apps or feature launches.

DEEP-DIVE & EXPERT SCENARIOS

If we use AI models trained on user data, what DPDP issues do we face? Map sections.

How does DPDP impact behavioural analytics tools like UEBA? Explain with examples.

DEEP-DIVE & EXPERT SCENARIOS

We use third-party tracking pixels. List DPDP risks and fixes.

Explain DPDP duties of a Significant Data Fiduciary. Add practical controls.

DEEP-DIVE & EXPERT SCENARIOS

Give me a full compliance plan for DPDP + GDPR alignment.