CIPP (CIPP/[VERIFY: track]) — One-Page Study Guide

A) Exam Snapshot

• Track: CIPP/[VERIFY: US, E, C, A, or CN] • Issuer: IAPP (International Association of Privacy Professionals)
• Blueprint/BoK: [VERIFY: CIPP track + BoK version]
• Format: multiple-choice, single best answer [VERIFY: item formats].
• Questions/time: 90 in 150 minutes [VERIFY: totals for your track].
• Scoring: scaled; passing score reported as 300+ [VERIFY: scoring scale].

B) Domain Weights

Domain	Weight
Domains	Varies by region; the official exam blueprint lists topic areas and question ranges (min/max). [VERIFY: download the official blueprint for your track].

C) Core Workflow (How the exam thinks)

• Start with jurisdiction and applicability; match facts to the right law.
• Classify the data and purpose; identify sensitive/special categories early.
• Name the roles: controller vs. processor (or equivalents) and the vendor chain.
• Choose the legal tool: lawful basis, consent model, or permitted use; document it.
• Run the lifecycle: collection, use, sharing, retention, deletion; test minimization.
• Check transparency and rights handling; confirm timing, deadlines, and exceptions.
• Validate safeguards: contracts, transfers, security, and accountability evidence.

D) High-Yield Concepts

• Definitions: personal data, processing, anonymization vs. pseudonymization [VERIFY: local terms].
• Role tests: controller/processor, service provider/third party; what contracts must say.
• Core principles: purpose limitation, minimization, accuracy, storage limits, security, accountability.
• Lawful bases and consent quality; withdrawal and recordkeeping.
• Notice requirements: content, timing, online tracking/cookies [VERIFY: track coverage].
• Rights: access, deletion, portability, objection; identity verification and deadlines.
• Sensitive data rules: biometrics, health, precise location, criminal data [VERIFY: track].
• Cross-border transfers: adequacy vs. SCCs vs. BCRs; onward transfer controls [VERIFY: region].
• Incidents: incident vs. breach; notification triggers and timing [VERIFY: jurisdiction].
• Enforcement basics: regulator powers, penalties, private rights of action [VERIFY: region].

E) Common Traps

• Picking “best practice” when the prompt asks “required by law” (or the reverse).
• Mixing jurisdictions or using the wrong statutory trigger for the fact pattern.
• Confusing notice with consent; a notice informs, consent authorizes (only sometimes).
• Assuming a vendor is a processor without testing purpose and discretion.
• Skipping exceptions and carve-outs (legal duty, litigation hold, investigations) [VERIFY: track].
• Treating pseudonymized data as anonymous, or ignoring identifiability context.
• For “best next step,” choosing a later action instead of jurisdiction/role/data-type first.

F) Cheat Sheet

• ROPA/data map; retention schedule; deletion log.
• DPIA/PIA and risk register entry.
• DPA/subprocessor list; audit rights; security exhibit.
• SCCs/BCRs; transfer impact assessment [VERIFY: track].
• Privacy/cookie notice; consent banner settings record.
• Rights intake log; ID verification record; response packet with rationale.

G) Exam-Day Tactics

• First pass: answer fast wins; mark long fact patterns.
• Underline the ask: lawful basis, notice timing, transfer tool, or enforcement trigger.
• Eliminate by definition: role, data type, jurisdiction, trigger condition.
• Watch absolutes (“always/never”) unless the law truly hard-codes it.
• Keep pace: about 1.5–1.7 minutes per question [VERIFY: your pacing].
• When stuck, choose the option that produces the strongest accountability record.
• Final sweep for blanks and marked items; change answers only with a clear reason.

H) 30-Minute Final Review Plan

• 0–5: roles and core definitions.
• 5–10: lawful bases/consent and notice timing.
• 10–15: rights workflow and deadline logic.
• 15–20: transfers toolkit (adequacy, SCCs, BCRs) [VERIFY: region].
• 20–25: breach triggers and who gets notified.
• 25–30: traps scan; commit to “jurisdiction → role → data type → tool → evidence.”