Data Privacy Impact Assessment

- A DPIA is a structured, documented process to identify and mitigate privacy risks
- Has moved from best practice to a core compliance obligation under GDPR, CCPA, and state laws
- Fits within privacy governance, product development, and regulatory accountability
- This course covers triggers, methodology, regulatory comparisons, operationalization, and review

PIA vs. DPIA: Terms, Roles, and Accountability

- **PIA**: broad global term; **DPIA**: GDPR Article 35 obligation with legal consequences

- **DPIA** is a preventive, forward-looking exercise, not retrospective paperwork

- Project or system owner holds responsibility, coordinated with privacy, legal, security, and DPO

The GDPR Trigger: High Risk Before Processing

- Article 35(1): DPIA required when processing is likely high risk to rights and freedoms

- Assessment completed before processing begins, not after launch

- Focus on new technologies and novel practices

- One assessment may cover similar high-risk processing operations

Article 35(3): Three Always-Mandatory Cases

Systematic and extensive automated evaluation, including profiling

Produces legal or similarly significant effects on individuals

Large-scale processing of special-category or criminal-offence data

RISK GATE

Systematic monitoring of publicly accessible areas on a large scale

These are mandatory floors, not limits—other high-risk processing may still require a DPIA

The EDPB Nine Criteria: Practical Screening

- Evaluation
- Scoring
- Automated decisions
- Systematic monitoring
- Sensitive data
- Large scale
- Dataset matching
- Vulnerable subjects
- Innovation
- Blocking services

- Evaluation, scoring, automated decisions, systematic monitoring
- Sensitive data, large scale, dataset matching, vulnerable subjects, innovation, blocking services
- Two criteria met? Conduct a DPIA; one severe can suffice
- Document all screening, even no-DPIA conclusions

National and Sectoral Additions to the Trigger

- Article 35(4) mandates national supervisory authority blacklists
- CNIL (France): whistleblowing and internal alert systems are always mandatory
- AP (Netherlands): employee camera surveillance and credit scoring trigger DPIAs
- Garante (Italy): systematic workplace email and internet monitoring
- Cross-border operations require checking every market's list
- One list is never sufficient for multi-country processing

US State Law Triggers and Divergences

- 15+ US states now mandate data protection assessments

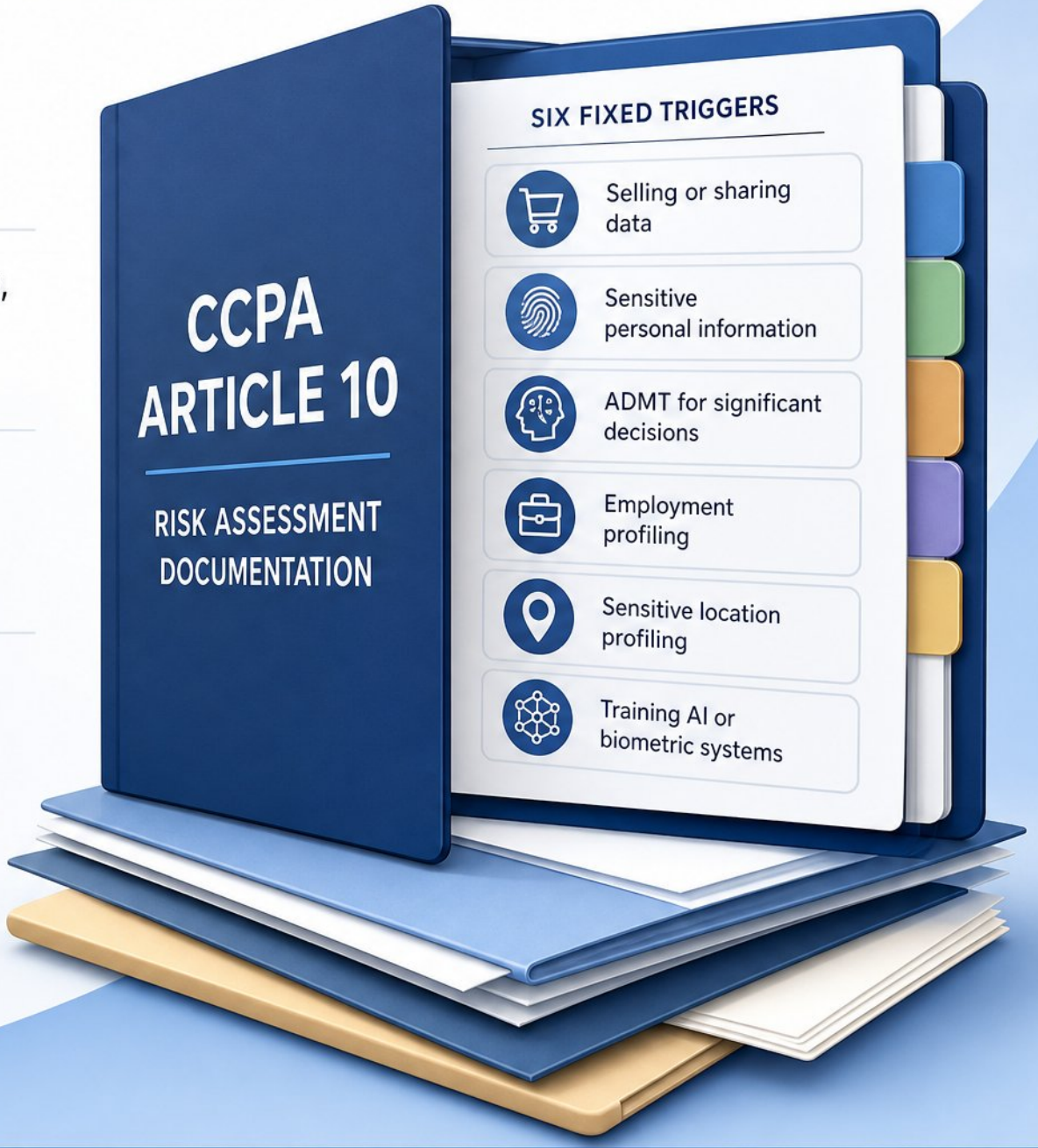
- Common triggers: targeted ads, data sales, profiling, sensitive data

- California's Article 10 is most prescriptive, with six trigger categories

- Regulatory submissions differ: CPPA filings vs. AG requests

CCPA Article 10: Risk Assessments in Practice

- Six fixed triggers include selling/sharing data, sensitive PI, ADMT for significant decisions
- Also covers employment profiling, sensitive location profiling, and training AI or biometric systems
- Documented balancing test weighs consumer privacy risks against business benefits
- Approval by a decision-maker; legal counsel may be excluded
- Continuous duties: 45-day material-change updates, 3-year refresh, CPPA submissions



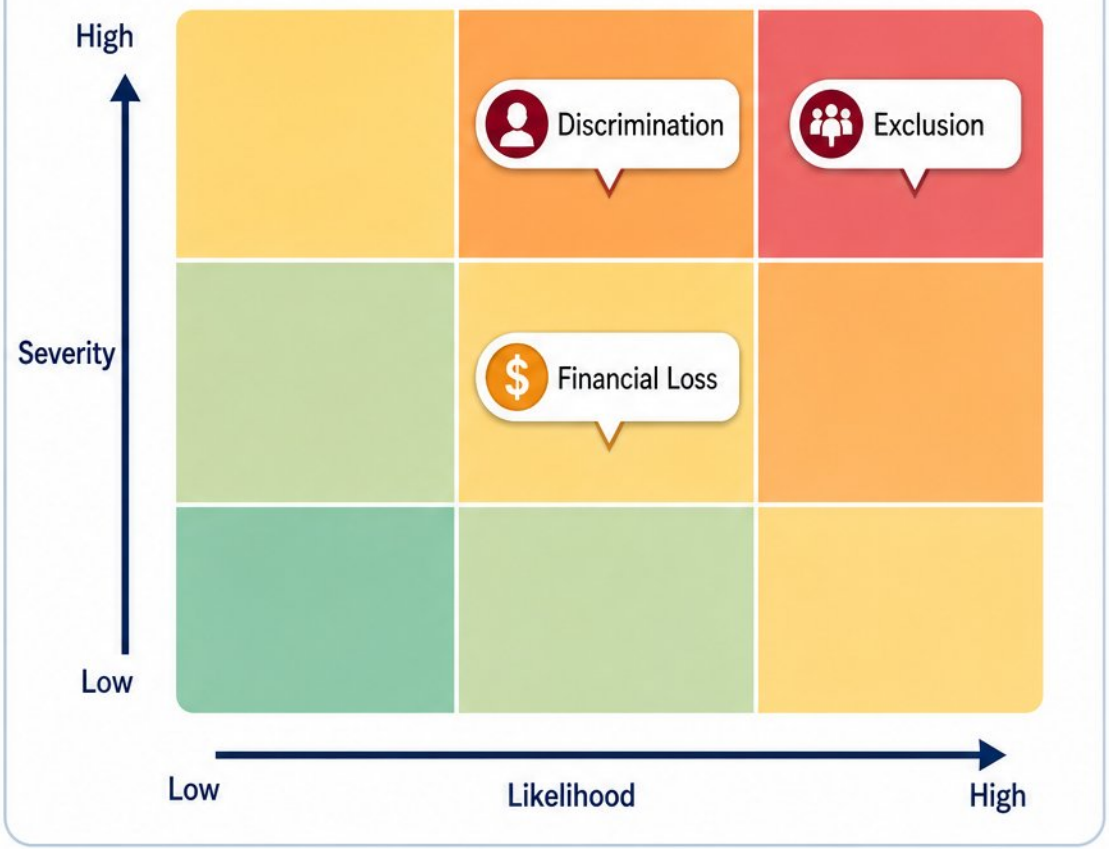
Core DPIA Content: Article 35(7) Minimums

- Describe the processing and purposes systematically
- Assess necessity and proportionality against minimization
- Evaluate risks to data subjects' rights and freedoms
- List safeguards, security, and compliance measures
- Document residual risk after mitigation

Risk Analysis: Method and Perspective

- Rate likelihood and severity of harm to individuals
- Assess across confidentiality, integrity, and availability
- Focus on rights-based harms: discrimination, financial loss, exclusion
- Include benefits; weigh residual risk after mitigation

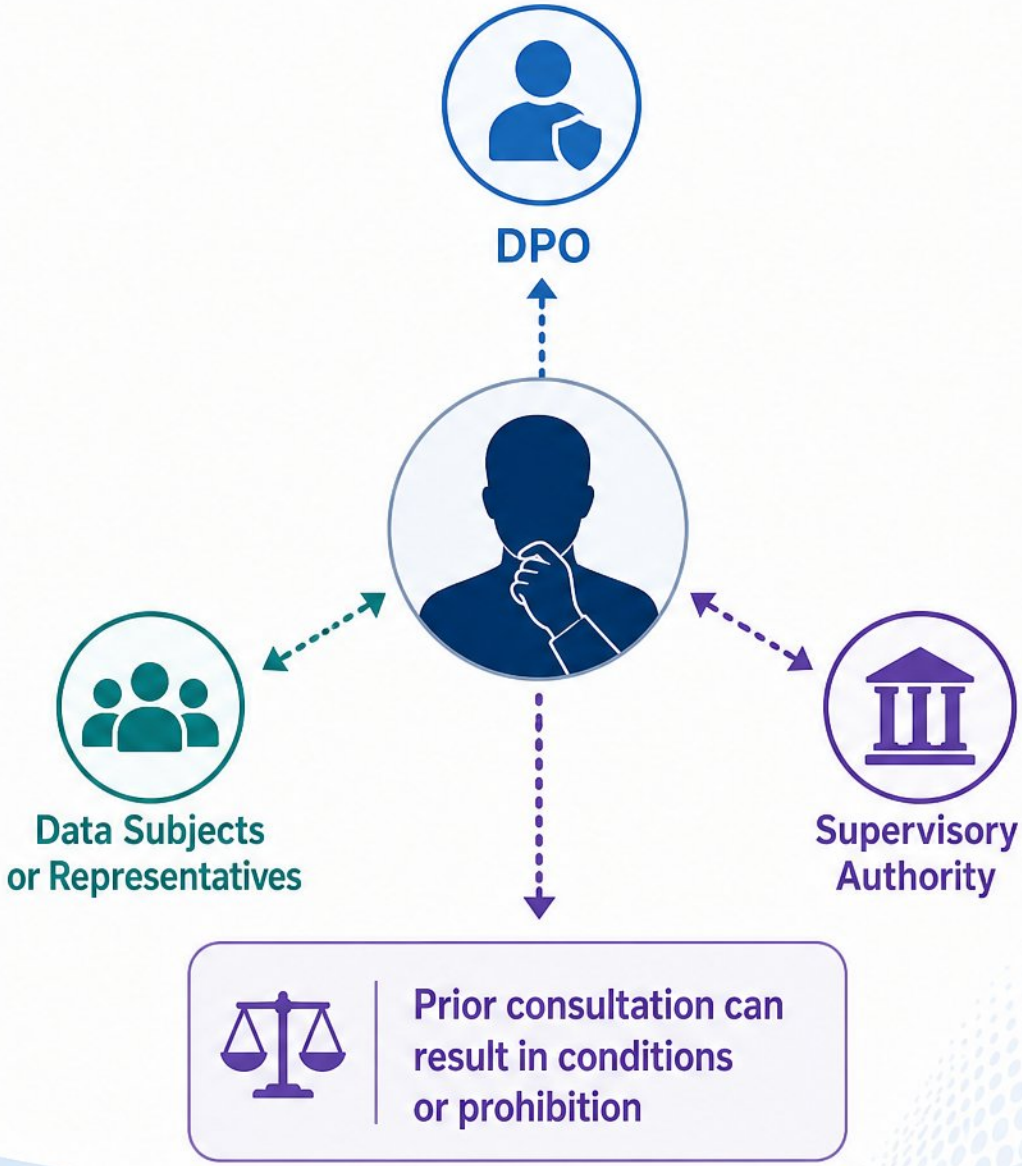
Likelihood–Severity Matrix (Individual Harm)



Analyze risk from the perspective of individuals and their rights. Balance potential harms with benefits to make responsible and human-centered decisions.

Consultation, DPO Advice, and Prior Consultation

- DPO advice required under Article 35(2), reviews but does not own the DPIA
- Seek data subject or representative input where appropriate
- Article 36: residual high risk triggers supervisory authority consultation
- Prior consultation can result in conditions or prohibition



Operationalizing DPIAs in the Development Lifecycle

- Embed screening into project intake with GDPR triggers and EDPB criteria
- National lists add mandatory cases per market
- Use a standardized template aligned to the 2026 EDPB structure
- Leverage existing data maps and records of processing
- Treat DPIAs as living documents tied to change management

The 2026 EDPB Template and AI Act Overlap

- EDPB adopted standardized DPIA template, March 2026
- Seven sections; default structure for new assessments
- National formats remain valid
- Coordinate DPIAs with AI Act fundamental rights impact assessments

AI ACT
FUNDAMENTAL RIGHTS IMPACT ASSESSMENTS

- Map impacts on fundamental rights
- Assess risks to vulnerable individuals
- Evaluate proportionality and safeguards
- Implement mitigations and ensure oversight

Practical Strategies for Programme Managers

- Screen at intake: two-plus EDPB criteria or one severe = DPIA before build
- Reuse data maps and processing records to prevent duplicate effort
- Document no-DPIA findings as accountability evidence
- Review on material change: data, vendors, models, regulations

PersonWise.

PersonWise • AI digital-human course platform

Scan the code or click anywhere to watch this course live, with voice Q&A

personwise.ai/t/049a760c/public