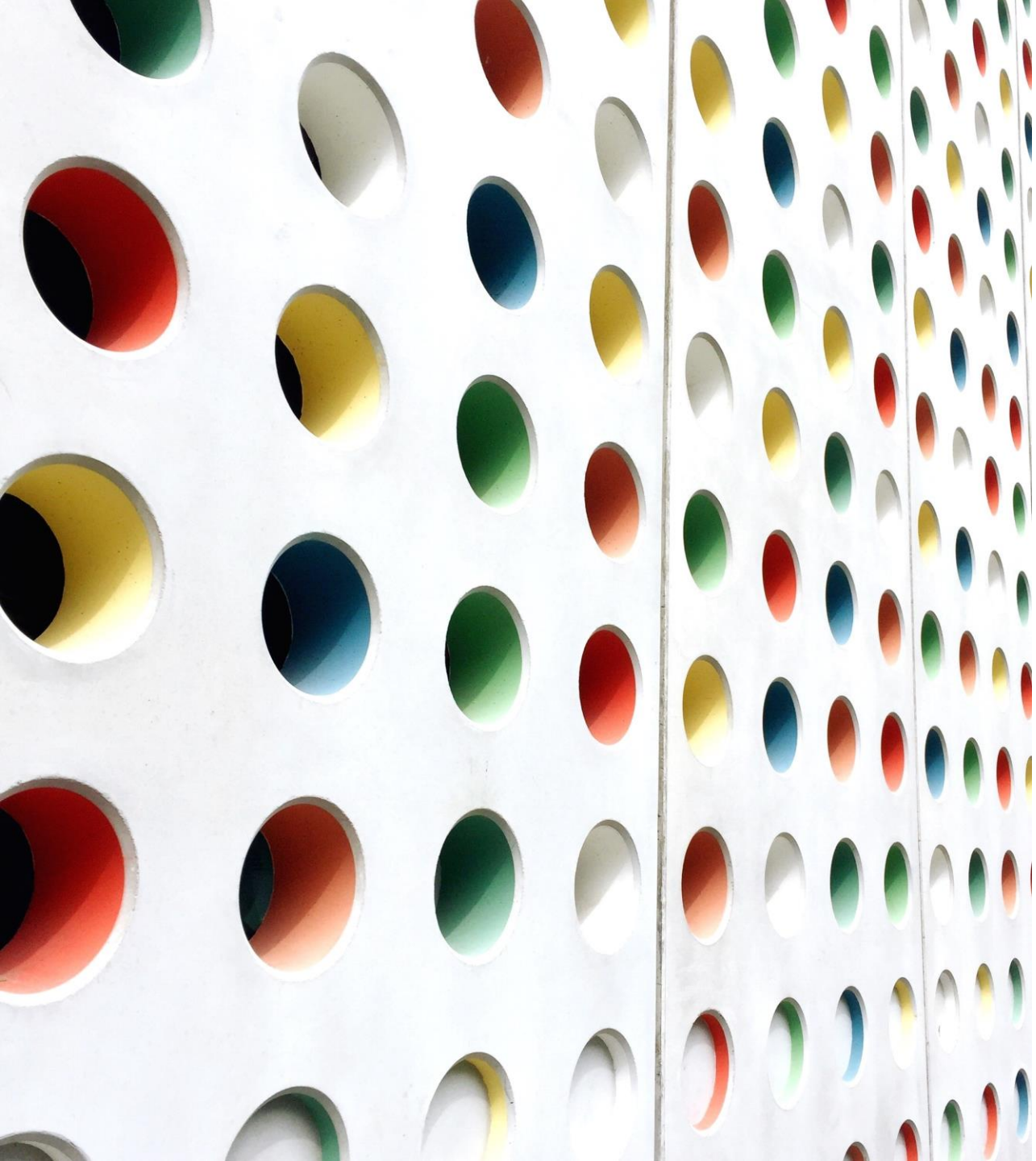
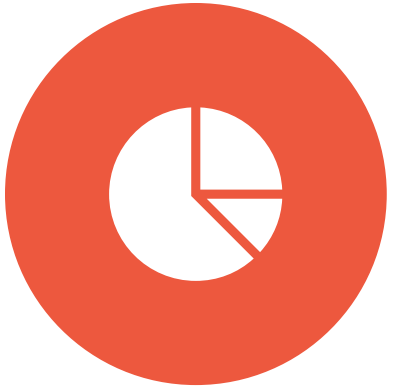


Cybersecurity Contracts

RAELLA DYKE, CYBERSECURITY & DATA PROTECTION ATTORNEY, CIPM, PMP, CISM, CISSP

CARLYN EPSTEIN, PRIVACY AND COMMERCIAL TRANSACTIONS ATTORNEY, CIPP

Cybersecurity: “the practice of defending devices, networks and data from malicious attacks or unauthorized exposure.”



DUE DILIGENCE: SECURITY PRACTICES IN PLACE.

CONTRACT TERMS: PRESERVE SECURITY PRACTICES, EXPECTATIONS FOR INCIDENTS

ONGOING OVERSIGHT: COMPLIANCE WITH CONTRACT TERMS AND INDUSTRY

Frequent Provisions: **Security Audit**

STANDARD TEXT

"Customer may audit Supplier for compliance with the terms of this Security Agreement. Supplier shall accommodate all Customer requests, including access to logs and on-site systems upon written request. Customer shall provide no more than 30 days notice. Customer may appoint a third-party auditor, who shall not be a competitor of Supplier, to conduct the audit. Any auditor shall sign an NDA with Supplier prior to commencement of the audit. Within 30 days of the final audit report, Supplier implement any remediation plans set out in the final audit report."

POSSIBLE REDLINES

- Scope to security concerns re: audits (documentation)
- Notice timeline
- Access limitations
- Resource demand, pricing model for extended audits
- Remediation requirements – scope, final determinant

Frequent Provisions: **Security Incident**

STANDARD TEXT

In the event of a confirmed or reasonably suspected Security Incident, Supplier shall notify Customer promptly (no later than 12 hours) after becoming aware of a Security Incident. Such Notification shall be provided in writing with a read-receipt to securityopscenter@Customer.com and by a call to Customer's 24/7 security hotline at 888-555-OOPS. Supplier shall reimburse Customer for all costs incurred as a result of the Security Incident. Supplier shall take all necessary and appropriate corrective actions, as instructed by Customer, to remedy any Security Incident.

POSSIBLE REDLINES

- definition of Security Incident
- notification window, depending on applicable laws / sensitivity of data
- notification trigger – "suspicion"
- costs of forensics and investigation
- remediation transparency
- notification and media restrictions
- scope to Privacy or Business Continuity concerns

Frequent Provisions: **“Flow-Down”**

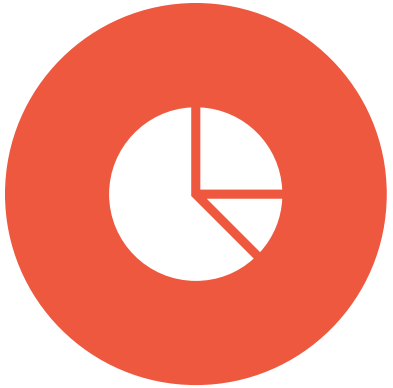
STANDARD TEXT

Supplier shall ensure all subcontractors and agents comply with the terms of this Agreement. Supplier shall conduct an annual audit or each subcontractor to ensure such compliance, and shall share these results with Customer upon request.

POSSIBLE REDLINES

- “applicable” – scope to services provided
- Substantive continuity throughout supply chain
- “proof of compliance” in lieu of audit results
- Oversight frequency commensurate with risk

Privacy: “the practice of protecting the rights of individuals to control their personal data”



DUE DILIGENCE: PRIVACY SAFEGUARDS IN PLACE

CONTRACT TERMS: PRIVACY LAW COMPLIANCE

ONGOING OVERSIGHT: COMPLIANCE WITH CHANGING PRIVACY LAWS, CONTRACT TERMS

Frequent Provisions: **Purpose Limitation**

STANDARD TEXT

PURPOSE LIMITATION

Supplier shall process the Personal Data in accordance with the Agreement, applicable SOW, and Customer's written instructions.

POSSIBLE REDLINES

There should be no redlines to this provision

- If Supplier can use Personal Data for its own purposes, you have "sale" problems under CCPA, Controller issues under GDPR

Frequent Provisions: **Data Subject Requests**

STANDARD TEXT

DATA SUBJECT REQUESTS

Supplier shall cooperate and assist Customer with responding to any requests by data subjects related to rights provided under applicable data protection law.

RIGHTS: access, deletion, rectification, portability

POSSIBLE REDLINES

- Self-service within system
- Timing/forwarding requests
- Exceptions to responding
- Paying for assistance

Frequent Provisions: **Cross-Border Transfer**

STANDARD TEXT

CROSS-BORDER TRANSFER

If Supplier processes Personal Data originating from the European Economic Area, the parties shall execute Standard Contractual Clauses prior to any processing.

POSSIBLE REDLINES

- Remove with affirmative statement no EEA Personal Data is involved
- Caution: called into question by opinion invalidating Privacy Shield
  - Current workaround relating to law enforcement policies

Frequent Provisions: **Liability**

STANDARD TEXT

INDEMNITY

Security Breach or violation of Supplier's data protection obligations
Special attention to fines brought by regulatory authorities

LIMITATION OF LIABILITY

Ideally uncapped, but otherwise in millions

POSSIBLE REDLINES

- Traditional indemnity replaced by covering costs of:
  - Mitigating Security Breach
  - Notifying data subjects and authorities
  - Credit monitoring, call centers
- Supercaps

Cybersecurity Standards & Resources:

Cyber certifications and frameworks:

- NIST Cybersecurity Framework or NIST 800-53
- ISO 27001 Certification
- SSAE 18 SOC II Type I and II
- PCI DSS
- NIST 800-88

Resources:

- ENISA – www.Europa.eu
- NIST – www.nist.gov/topics/cybersecurity
- Cybersecurity Law Report – www.Cslawreport.com

Privacy Resources:

Resources

- International Association of Privacy Professionals (IAPP) – iapp.org
- DLA Piper Data Protection Laws of the World – dlapiperdataprotection.com
- Electronic Frontier Foundation (EFF) – eff.org/issues/privacy
- Government entities/enforcement
  - Federal Trade Commission (US)
  - Information Commissioner's Office (UK)
  - California Attorney General