Källor

Allmänna dataskyddsförordningen, dvs. GDPR (på alla språk, i HTML- eller PDF-format), i synnerhet artiklarna:

- 2 (materiellt tillämpningsområde)
- 4 (definitioner)
- 5 (principer för behandling av personuppgifter)
- 6 (behandlingsgrunderna)
- 7–8 (villkor för samtycke)
- 9 (behandling av särskilda kategorier av personuppgifter)
- 12 (skyldighet att informera den registrerade om behandlingen och den registrerades rättigheter)
- 13 (information som ska ges då personuppgifter samlas in från den registrerade)
- 14 (information som ska ges då personuppgifter samlas in från någon annan källa)
- 15 (rätt till tillgång och en checklista över information som ska ges då den registrerade vill veta hur hens uppgifter behandlas)
- 16 (rätt till rättelse)
- 17 (rätt till radering, det vill säga ”rätten att bli bortglömd”)
- 18 (rätt till begränsning av behandling)
- 19 (anmälningsskyldighet då uppgifter rättas eller raderas)
- 21 (rätt att göra invändningar)
- 25 (inbyggt dataskydd och dataskydd som standard)
- 30 (register över behandling)
- 32 (säkerhet i samband med behandlingen)
- 33–34 (förfarande vid personuppgiftsincidenter)

Beredningsdokumenten för dataskyddslagen (lagen har ännu inte publicerats på Finlex), i synnerhet:

- 4 § (tillämpning av allmänt intresse som behandlingsgrund)
- 5 § (åldersgränsen för barns samtycke till informationssamhällets tjänster är 13 år)
- 6 § (grunder för behandling av särskilda kategorier av personuppgifter)
- 25 § (administrativa påföljdsavgifter gäller inte myndigheter)
- 27 § (behandling för journalistiska, akademiska, konstnärliga eller litterära ändamål)
- 28 § (offentlighetsprincipen inskränks inte genom GDPR, jfr dock 16 § 3 mom i lagen om offentlighet i myndigheternas verksamhet)
- 29 § (behandling av personbeteckningar)
- 34 § (begränsningar i rätten att få tillgång till uppgifter)

Europeiska dataskyddsstyrelsens (EDPB) riktlinjer, beslut och rekommendationer (mest på engelska)

Dataombudsmannens informationsresurser för personuppgiftsansvariga

Checklista för implementeringen av GDPR

Steg 1: Reflektion

- Vilka personuppgifter (art. 4) behandlar vi gällande elever/studerande respektive vårdnadshavare?
- Vilka särskilda kategorier av personuppgifter (art. 9) behandlar vi?
- Varför behandlar vi olika personuppgifter, dvs. hur definierar vi ändamålet (art. 5)?
- Kan man dela in behandlingen i logiska helheter enligt ändamål?
- Vilken är behandlingsgrunden (art. 6) för personuppgifter i allmänhet och för särskilda kategorier i synnerhet? (Behandlingsgrunderna kan vara olika inom olika logiska helheter.) Finns det behandling som kräver samtycke (art. 7–8)?
- Varifrån och hur samlas uppgifterna in?
- Hur och när informerar vi de registrerade (art. 12–14) – vårdnadshavare och barn – om hur vi behandlar deras personuppgifter och om deras rättigheter?
- Var finns personuppgifterna?
- Vem har tillgång till personuppgifterna?
- Hur länge sparas personuppgifterna och vad händer när de inte längre behövs?
- När lämnar vi ut personuppgifter till en tredje part?
- Vem tar bollen när en registrerad vill utöva sina rättigheter till tillgång, rättelse, radering, begränsning av behandlingen och invändningar (art. 15–22)? Hur går det till?
- Vilka tekniska och organisatoriska åtgärder har vi vidtagit för att skydda uppgifterna (art. 32)? Är de tillräckliga?
- Vilka är riskerna med behandlingen (art. 25)? Krävs det en konsekvensbedömning (art. 35)?
- Hur går vi tillväga om det sker en personuppgiftsincident (art. 33–34)? Vem gör vad?

Steg 2: Dokumentation (mer utförligt på Dataombudsmannens webbplats)

- Har vi ett register över behandling (art. 30) (inte en registerbeskrivning av tidigare slag)?
- Har vi koncisa, tydliga och begripliga informationstexter avsedda för de registrerade (art. 12) som innehåller den information som räknas upp i art. 13–14? Är språket klart och tydligt, särskilt med beaktande av barn som målgrupp? Är de tillgängliga, så att man inte behöver fråga efter dem?
- Har vi (interna) processbeskrivningar för hur vi går tillväga
    - då en registrerad vill utöva sina rättigheter till tillgång, rättelse, radering, begränsning av behandlingen och invändningar (art. 15–22)
    - då en registrerad vill återta sitt samtycke (om behandlingsgrunden är samtycke) (art. 7)
    - då det sker en personuppgiftsincident (art. 33–34)?
- Om behandlingsgrunden för någon behandling är samtycke, kan vi påvisa att samtycke finns?
- Har vi dokumentation över de tekniska och organisatoriska åtgärder som har vidtagits för att skydda personuppgifterna (art. 32)?
- Har vi gjort en riskanalys (art. 25)?

Steg 3: Kontinuitet

- Hur utbildar vi vår personal i frågor som gäller dataskydd?
- Har vi utnämnt ett dataskyddsombud (art. 37–39)? Vet personalen vem det är?
- Hur ofta utvärderar vi dataskyddet inom vår organisation? Vem ansvarar för det?