Aluehallintovirasto
Regionförvaltningsverket
Regional State Administrative Agency

GDPR – definition och hur utbildningen berör(t)s av förordningen

Tammerfors 29.11.2018

Thomas Sundell

Jurist

Regionförvaltningsverkens
svenska enhet för bildningsväsendet

GDPR som lagstiftning

- Står för General Data Protection Regulation, det vill säga EU:s allmänna dataskyddsförordning (2016/679), som kan hittas här: https://eur-lex.europa.eu/legal-content/SV/ALL/?uri=celex%3A32016R0679
- Godkändes 25.5.2016 och trädde i kraft 25.5.2018
- Gäller i egenskap av EU-förordning direkt och behöver inte implementeras nationellt såsom EU-direktiv
  - Nationell lagstiftning får inte vara i konflikt med GDPR
- Dataskyddslagen godkändes i riksdagen 13.11.2018 och kompletterar med det som får bestämmas nationellt

Hur stor ändring är det fråga om?

- Syftet med GDPR är inte att förhindra behandling av personuppgifter utan att göra den mer strukturerad, genomtänkt och transparent
- Åtminstone i Finland har det gjorts mängder av verksamhetshämmande övertolkningar – GDPR säger oftast inte rakt av vad man får eller inte får göra, utan det handlar om huruvida man kan motivera det
- Om man hade följt den gamla personuppgiftslagen skulle förändringen inte vara fullt lika stor
- Viktigare med reflektion över verksamheten än juristeri

Tillämpningsområde

- GDPR tillämpas på behandling av personuppgifter som är helt eller delvis automatisk samt manuell behandling där uppgifterna ingår i eller kommer att ingå i ett register
- Tillämpas inte på behandling som en fysisk person utför i rent privata syften eller i samband med sitt hushåll
- Tillämpas i begränsad utsträckning på behandling för journalistiska, akademiska, konstnärliga eller litterära ändamål
- Gäller både elevernas, vårdnadshavarnas och personalens uppgifter

Personuppgifter, register och behandling

- § Personuppgifter är ”varje upplysning som avser en identifierad eller identifierbar fysisk person”
- § Ett register är ”en strukturerad samling av personuppgifter som är tillgänglig enligt särskilda kriterier”
- § Behandling innefattar allt man kan göra med personuppgifter, både manuellt och automatiskt, inklusive att samla in, ta del av på olika sätt, ändra, lämna ut och radera dem

Roller

- Personuppgiftsansvarig (rekisterinpitäjä) = den som primärt behandlar uppgifter, tidigare ”registeransvarig”
  - Flera organisationer kan också ansvara gemensamt
- Personuppgiftsbiträde (henkilötietojen käsittelijä) = den som behandlar uppgifter på uppdrag av den personuppgiftsansvariga
- Dataskyddsombud (tietosuojavastaava) = en utnämnd person som ska handleda den personuppgiftsansvariga i GDPR-frågor och internt övervaka att man följer reglerna
- Dataombudsmannen (tietosuojavaltuutettu) = den tillsynsmyndighet som övervakar att GDPR efterlevs

Principerna för dataskydd

- § Laglighet, korrekthet och öppenhet
- § Ändamålsbegränsning
- § Uppgiftsminimering
- § Lagringsminimering
- § Korrekthet
- § Integritet och konfidentialitet
- § Ansvarsskyldighet
- § Privacy by design

Behandlingsgrunder

§ All behandling måste bygga på en behandlingsgrund:

- Samtycke
- Fullgörande av avtal där den registrerade är part
- Fullgörande av rättslig förpliktelse (lakisääteinen velvoite)
- Skydd av intressen som är av grundläggande betydelse för den registrerade eller någon annan fysisk person (elintärkeiden etujen suojaaminen)
- Utförande av uppgift av allmänt intresse eller som ett led i myndighetsutövning (julkisen vallan käyttö)
- Den personuppgiftsansvariges eller tredje parts ”berättigade intressen”, om inte den registrerades intressen, rättigheter och friheter väger tyngre (kan inte tillämpas av myndigheter)

Samtycken

- Om behandlingen grundar sig på samtycke måste samtycket kunna bevisas och det måste vara en aktiv handling (t.ex. kryss i en ruta, men inte icke-kryss)
- Om samtycket gäller flera ändamål ska man få välja
- Begäran om samtycke måste läggas fram så att den tydligt kan särskiljas, i en begriplig och lättillgänglig form och med klart och tydligt språk
- Samtycket måste vara frivilligt – det kan när som helst återkallas och man måste informera om möjligheten
- Man kan inte samtycka till något som är helt onödigt

Barn och informationssamhällets tjänster

- Enligt GDPR kan barn under 16 år inte själva samtycka till behandling av personuppgifter i fråga om det som kallas ”informationssamhällets tjänster” (i praktiken t.ex. molntjänster, sociala medier och olika appar), utan för dessa krävs vårdnadshavarnas samtycke
- Medlemsstaterna får dock sänka åldersgränsen ända till 13 år, vilket Finland har gjort i dataskyddslagen
- Personuppgiftsansvariga ska göra rimliga ansträngningar för att kontrollera vårdnadshavarens samtycke

Särskilda kategorier av personuppgifter

- Det som förr kallades känsliga personuppgifter heter i GDPR ”särskilda kategorier av personuppgifter” (9 art.)
- Det är förbjudet att utan lagstadgad grund eller samtycke
  - behandla personuppgifter som avslöjar ras eller etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse eller medlemskap i fackförening
  - behandla av genetiska uppgifter, biometriska uppgifter för att entydigt identifiera en fysisk person, uppgifter om hälsa eller uppgifter om en fysisk persons sexualliv eller sexuella läggning
- Fotografier är inte i sig biometriska uppgifter (skäl 51)
- Uppgifter om brott och straff har en särställning (10 art.)

Information om behandlingen

- § Den personuppgiftsansvarige ska ge information om principerna för behandlingen och hur den registrerade utövar sina rättigheter enligt förteckningar i artiklarna 13 (då uppgifter samlas in av den registrerade) och 14 (då uppgifter om den registrerade samlas in annanstans)
- § Informationen ska ges i en koncis, klar och tydlig, begriplig och lättillgänglig form och med ett klart och tydligt språk, särskilt då den riktas till barn
- § Informationen ska vara skriftlig och kan vara i elektronisk form där det är lämpligt

Den registrerades rättigheter

- § Den registrerade har rätt till 1) tillgång, 2) rättelse, 3) radering, 4) begränsning av behandling och 5) dataportabilitet (punkt 5 gäller inte myndigheter)
- § Den personregisteransvarige ska utan dröjsmål men senast inom en månad meddela vilka åtgärder som vidtagits med anledning av en begäran
- § Om inga åtgärder vidtas ska den registrerade meddelas om orsaken och möjligheten att söka ändring
- § Utövandet av rättigheterna ska vara gratis om inte begäran är uppenbart ogrundad eller orimlig

Dokumentering av behandlingen

- Det är viktigt att kunna påvisa att man beaktar GDPR och har vidtagit nödvändiga åtgärder
- Dokumentationen består till exempel av:
  - Register över behandling enligt 30 art. (gäller myndigheter och sådana organisationer som sysselsätter fler än 250 personer eller som behandlar särskilda kategorier av personuppgifter)
  - Den information som ges till de registrerade
  - Eventuella samtycken
  - Processbeskrivningar och instruktioner
  - Avtal om ansvarsfördelning
  - Avvikelser från dataskyddsombudets rekommendationer

Tillsyn

- Dataombudsmannen fungerar som tillsynsmyndighet
- Tillsynsmyndigheten kan begära information och göra inspektioner på eget initiativ eller på basis av klagomål
- Tillsynsmyndigheten kan ge varningar, reprimander och förelägganden om att rätta brister
- Den strängaste och mest omtalade påföljden är de administrativa sanktionsavgifterna, som kan ges i stället för eller utöver de korrigerande åtgärderna
  - Enligt dataskyddslagen gäller detta inte myndigheter

Skyldighet att anmäla incidenter

- § Personuppgiftsincidenter måste utan dröjsmål och om möjligt inom 72 timmar anmälas till tillsynsmyndigheten om det inte är osannolikt att incidenten får några följder
  - Vid förseningar måste förseningen motiveras
  - Innehållet i anmälan listas i artikel 33
- § Om incidenten sannolikt leder till en hög risk för fysiska personers intressen ska också registrerade informeras, i första hand personligen men annars via allmänheten

Ersättningsskyldighet

- § Den som har lidit materiell eller immateriell skada till följd av brott mot GDPR har rätt till ersättning
- § I tidigare PUL tillämpades strikt ansvar – ersättning utgick oberoende av om någon hade gjort något fel – men i GDPR gäller vållande med omvänd bevisbörda: den personuppgiftsansvariga ska visa att den inte på något sätt är ansvarig för händelsen som orsakat skada
- § Personuppgiftsansvariga och personuppgiftsbiträden som har medverkat i samma behandling är solidariskt ansvariga

Personuppgifter inom utbildningen

- Elevernas och vårdnadshavarnas uppgifter finns t.ex. i elevregister, elevhälsoregister, i olika blanketter och på olika håll i den dagliga verksamheten
  - Behandlingen borde beskrivas, och behandling som inte fyller några administrativa eller pedagogiska syften borde elimineras
- Vissa gånger kräver lagen behandling, vissa gånger är det motiverat med tanke på verksamheten och vissa gånger något ”extra” som ändå fyller ett syfte
- Också arkiveringen påverkas av GDPR