Datskyddsförordningen – Gymnasieantagning

Stockholm och Göteborg oktober 2018

Staffan Wikell
Avdelningen för juridik

GDPR började gälla i hela EU den 25 maj 2018

- EU:s dataskyddsförordning (EU) 2016/679 av den 27 april 2016 (GDPR) började gälla samtidigt i alla medlemsländer. PuL upphörde att gälla. Den ersattes av dataskyddslagen (2018:218)
- Skärpt ansvar och skyldigheter för personuppgiftsansvariga organisationer
- Utökade rättigheter för registrerade individer
- Syftet med reglerna är detsamma som i PUL :
  - att skydda fysiska personers integritet vid behandling av deras personuppgifter

Hierarkin mellan författningarna

När är dataskyddslagstiftningen tillämplig?

- Lagstiftningen omfattar inte bara stora IT-system utan även information i word/excel som ligger på en anställds egen hårddisk eller serverutrymme.
- Det finns ingen ”privat” behandling inom ramen för myndighetens verksamhet.
- Definitionen av ”personuppgift” är väldigt vid.

Personupgiftsansvarig

– Den som ensam eller tillsammans med andra bestämmer ändamålen och medlen för behandlingen av personuppgifter. Artikel 4 p 7. Krävs inga beslut. Ansvaret följer direkt av lagens definitioner.

– Gemensamt personuppgiftsansvar är möjligt enligt artikel 26 GDPR.

Nytt! Den personuppgiftsansvarige ska ha en registerförteckning. Artikel 30

- Den personuppgiftsansvarige (PuA) måste hålla ett register över alla behandlingsändamål i sin verksamhet, både för strukturerad och ostrukturerad behandling. Artikel 30.
- Den ska innehålla, namn och kontaktuppgifter för PuA och för dataskyddsombudet, ändamål med behandlingen, kategorier av registrerade, kategorier av personuppgifter, kategorier av mottagare av uppgifter, om uppgifter överförs till tredje land och vilket land det är, om möjligt bevarandetid för personuppgifter, och en allmän beskrivning av säkerhetsåtgärder.
- Idag gäller en likadan skyldighet för personuppgiftsombudet. Ostrukturerad behandling av personuppgifter omfattas inte.
- SKL har tagit fram en mall för hur förteckningen kan se ut, ligger på hemsidan skl.se.

Nytt. En PuA och ett PuB är skyldig att utse ett dataskyddsombud om..

En personuppgiftsansvarig och ett personuppgiftsbiträde ska utnämna ett dataskyddsombud

- Om behandlingen utförs av en myndighet eller ett offentligt organ (artikel 37, p. 1 a)
- Om kärnverksamheten består av behandling av personuppgifter som kräver regelbunden och systematisk övervakning av de registrerade i stor omfattning (artikel 37, p. 1 b) .
- Om kärnverksamheten består av behandling i stor omfattning av känsliga personuppgifter eller som rör fällande domar i brottmål och överträdelser enligt art 10 (artikel 37, p. 1 c) m.m.
- Flera PuA kan dela på ett DSO. Varje myndighet måste i så fall förordna samma person.

Nytt:En PuA ska till Datainspektionen anmäla en inträffad personuppgiftsincident

- En PuA som drabbas av en personuppgiftsincident måste anmäla den till Datainspektionen, om möjligt, senast inom 72 timmar från det att man fick vetskap om att den inträffat. Det kan ha skett genom dataintrång (brottsligt angrepp) eller utlämnande eller förstöring av uppgifter, genom slarv el olyckshändelse.
- Förordningen innehåller krav på vad incidentrapporten ska innehålla och att rapporten ska sparas, vilket tillsammans med den korta tidsfristen, gör att man måste ha rutiner på plats för att utreda, dokumentera, rapportera en sådan incident. T ex bör ansvaret för att göra en anmälan om inträffad incident pekas ut i organisationen.
- Om det är osannolikt att en inträffad incident medför risk för de registrerades integritet så behöver anmälan inte göras.
- Om incidenten kan leda till allvarliga risker för de registrerades integritet så ska också de registrerade som drabbats informeras om händelsen.

Nyheter: Konsekvensbedömning avseende dataskydd. Artikel 35

- Om behandling av personuppgifter planeras och den sannolikt leder till hög risk för enskildas friheter och rättigheter ska den PuA göra en konsekvensbedömning avseende dataskyddet.
- Det kan handla om behandling i stor omfattning av känsliga personuppgifter, en systematisk bedömning av fysiska personers personliga egenskaper inbegripet profilering eller systematisk kameraövervakning av allmän plats.
- Samråd med Datainspektionen ska göras.
- Datainspektionen ska komma med vägledning om vilka typer av behandling som ska omfattas av kravet på konsekvensbedömning.

Personuppgiftsbiträde ?

- Personuppgiftsbiträde (PuB) är en extern part vars uppgift är att behandla personuppgifter på uppdrag av en PuA, behandlingen ska vara för PuA:s räkning. I annat fall ej PuB.
- Om en part lämnar ut personuppgifter till en annan part medför det inte automatiskt att biträdesavtal ska tecknas. Det krävs att mottagaren av personinformationen ska behandla uppgifterna för den utlämnandes räkning, och inte för sin egen räkning.

Nyheter: utvidgade krav på avtalen med personuppgiftsbiträden. Artikel 28

- Personuppgiftsbiträde är en som behandlar personuppgifter för den PuA:s räkning. Särskilt biträdesavtal ska finnas.
- Ett biträde måste i avtalet kunna ge tillräckliga garantier om att genomföra lämpliga tekniska och organisatoriska åtgärder, på sådant sätt att behandlingen uppfyller förordningens krav och att man säkerställer att de registrerades rättigheter skyddas.
- För att biträdet ska få anlita ”underbiträden” krävs ett särskilt eller allmänt skriftligt förhandstillstånd från den PuA. Om ett allmänt förhandstillstånd erhållits ska biträdet informera PuA om eventuella planer på att anlita nya underbiträden så att PuA kan göra invändningar mot förändringen.
- Biträdet ska i avtalet säkerställa att alla personer hos biträdet med behörighet att behandla personuppgifter har åtagit sig att iaktta konfidentialitet eller omfattas av lämplig lagstadgad tystnadsplikt.

Nyheter: utvidgade krav på avtalen med personuppgiftsbiträden. Artikel 28

- Avtalet ska innehålla att biträdet ska hjälpa den PuA med att se till att skyldigheterna i artiklarna 32-36 fullgörs.
- Avtalet ska innehålla att biträdet, vid avtalets upphörande, ska beroende vad den PuA väljer, radera eller återlämna alla personuppgifter till den PuA, och radera alla befintliga kopior såvida inte lagring fortsatt krävs enligt unionsrätten eller nationell rätt i medlemsstaten.
- Om personuppgiftsbiträdet anlitar underbiträden för utförande av specifik behandling på PuA:s vägnar så ska det biträdet genom avtal åläggas samma skyldigheter ifråga om dataskydd som det som gäller i avtalet mellan PuA och PuB. Om underbiträdet inte fullgör sina skyldigheter ifråga om dataskyddet så ska PuB vara fullt ansvarig gentemot PuA för utförandet av underbiträdets skyldigheter

Den registrerades rättigheter – vad är nytt?

- Samtycket ska vara tydligare och krävs oftare (?)
- Informationskravet blir ännu mer omfattande
- Registerutdrag ska kunna lämnas elektroniskt
- Rätten att bli glömd, återkalla samtycke, rättelse, registerutdrag m.m.
- Dataportabilitet
- Rätt till notifiering vid incidenter

Grunder för laglig behandling, artikel 6

- Grund för behandling av personuppgifter. Någon av de grunder som räknas upp I artikel 6, 1. a-f måste vara tillämplig. I stort sett samma grunder som i 10 § PuL.

- a, den registrerades samtycke
- b, behandlingen är nödvändig för fullgörande av avtal mellan den registrerade och den personuppgiftsansvarige ,
- c, ….. nödvändig för att fullgöra en rättslig förpliktelse som åvilar den personuppgiftsansvarige,
- d, …nödvändig för att skydda intressen av grundläggande betydelse för den registrerade eller annan
- e, nödvändig för att utföra en uppgift av allmänt intresse eller som led I den personuppgiftsansvariges myndighetsutövning …
- f, eller nödvändig för berättigade intressen hos den personuppgiftsansvarige eller hos tredje part efter en intresseavvägning mot den registrerades intresse att inte vara registrerad.

Grunder för laglig behandling artikel 6

För kommuner och landsting är de viktigaste grunderna art. 6, punkt 1. c och e. Behandlingen är nödvändig för…

- fullgörande av en rättslig skyldighet som åvilar den PuA
- utförande av en uppgift av allmänt intresse eller
- som led i den PuA:s myndighetsutövning.

- Kompletterande nationell lagstiftning för precisering av laglig grund krävs. (Dataskyddslagen)

Ny dataskyddslag

kompletterande svenska bestämmelser

- En lag om dataskydd som kompletterar EU:s dataskyddsförordning i vissa delar. Bestämmelserna har generell karaktär, de rör en hel sektor eller hela samhället.
- ”Sektorsspecifika nationella lagar/förordningar om dataskydd ska ha företräde framför ”dataskyddslagen”. Finns idag mer än 150 sådana författningar.
- Förhållandet till våra grundlagarna ändras inte. Undantag görs för tryck-och yttrandefriheten
- Lagen preciserar rättsliga grunder för behandling när det gäller ”rättslig förpliktelse”, ”uppgift av allmänt intresse” och ”som ett led i myndighetsutövning”, artikel 6.1. c) och e)

Ny dataskyddslag

Rättslig grund för behandling av personuppgifter

– 2 kap 1 §. Personuppgifter får behandlas med stöd av art 6.1 c i dataskyddsförordningen om behandlingen är nödvändig för att den personuppgiftsansvarige ska kunna fullgöra en **rättslig förpliktelse** som 1. gäller enligt lag, annan författning 2 följer av kollektivavtal eller 3. följer av beslut som meddelats med stöd av lag.

– 2 kap 2 § . Personuppgifter får behandlas med stöd av art 6.1 e dataskyddsförordningen om behandlingen är nödvändig 1.) för att utföra en uppgift av **allmänt intresse** som följer av lag eller annan författning, av kollektivavtal eller av beslut som har meddelats med stöd av lag eller annan författning, eller 2.) som ett led i den

Känslig information

Förbjudet att registrera – men det finns många undantag

- ras eller etniskt ursprung
- politiska åsikter
- religiös eller filosofisk övertygelse
- medlemskap i fackförening
- hälsa
- sexualliv, sexuell läggning
- genetisk och biometrisk information (GDPR)

Känslig information – exempel undantag

- uttryckligt samtycke
- arbetsrätten (även kollektivavtal i GDPR)
- socialtjänst/socialförsäkring
- skydda vitala intressen
- ideella organisationer
- eget offentliggörande
- viktigt allmänt intresse (nytt)
- hälso- och sjukvård
- allmänt intresse på folkhälsoområdet (nytt)
- arkivering (nytt), forskning och statistik
- rättsliga anspråk

Ny dataskyddslag

Behandling av känsliga personuppgifter

- Undantag från förbudet mot behandling av känsliga personuppgifter görs inom **hälso- och sjukvård** och **socialtjänst** (3 kap 5 §), inom **arbetsrätten** (3 kap 2 §), för **arkivändamål av allmänt intresse** (3 kap 6 §), **statistik** (3 kap 7 §). Gäller myndigheter och andra PuA,
- **Viktigt allmänt intresse**. Undantag i myndigheters verksamheter generellt, dels nödvändig behandling vid **ärendehandläggning**, dels om **uppgiften har lämnats till myndigheten och behandling krävs enligt lag** och dels **i annat fall om behandlingen är nödvändig m hänsyn till viktigt allmänt intresse och inte innebär otillbörligt intrång i den registrerades personliga integritet**. (3 kap 3 §). Obs, sökbegränsningar!
- Kommunala företag som omfattas av offentlighetsprincipen, får behandla känsliga personuppgifter om uppgiften lämnats till myndigheten och behandling krävs enligt lag (3 kap 3 § andra st) .

Personnummer

– Medlemsländerna får bestämma när nationellt ID-nummer får behandlas.

– Personnummer och samordningsnummer får behandlas utan samtycke endast när det är klart motiverat med hänsyn till ändamålet med behandlingen , vilkten av säker identifiering eller annat beaktansvärt skäl. 3 kap 10 § dataskyddslagen.

– Samma regel , samma möjligheter och begränsningar, som i PuL.

Krav på informationssäkerhet i GDPR

- Förordningen bygger på att den PuA själv ska bestämma informationssäkerhetskraven för behandlingen. Grunden i GDPR är ett riskbaserat angreppssätt
- Informationssäkerhet går ut på bevarande av informationens sekretess/konfidentialitet –riktighet –tillgänglighet och spårbarhet.
- Den PuA och biträdet ska vidta lämpliga tekniska och organisatoriska åtgärder för att säkerställa en lämplig säkerhetsnivå, artikel 32 GDPR.

Krav på informationssäkerhet i GDPR-Nyheter

- Inbyggt dataskydd och dataskydd som standard, privacy by design , privacy by default. Artikel 25.
- SKL har tagit fram verktyget KLASSA för informationsklassning för att hitta rätt informationssäkerhet.
- https://skl.se/naringslivarbetedigitalisering/digitalisering/informationssakerhet/klassainformationsklassning.7558.html

Personuppgifter i e-posten

- E-postsystemet skall finnas med i registerförteckningen. Ändamålet är att skicka och ta emot e-post. Det är inget diarium eller ärendehanteringssystem. Ej lämpligt för långtidslagring.
- Bevarandetiden eller kriterierna som bestämmer bevarandet ska anges i förteckningen. Den ska fastställas utifrån ändamålet med behandlingen.

Personuppgifter i e-posten

- Arkivlagen är överordnad GDPR bevarandefrågor och gallringsbeslut ska fattas med stöd av den lagen. Ingen skillnad mot tidigare.
- Till myndigheten inkommen e-post ska gås igenom. Mejl som hör till ett ärende ska flyttas till ett ärendehanteringssystem. Bra att ha är inget godtagbart skäl att spara inkomna mejl på sitt e-postkonto i myndigheten.
- Inkommen e-post som är allmän handling får bevaras enligt regler om offentlighetsprincipen och arkivlagen. Men ska enligt DI inte bevaras långsiktigt i epostsystemet. Gallringsbeslut för e-post ska finnas som för alla andra handlingsslag.
- Utgående mejl som innehåller känsliga personuppgifter. Krypterad e-post bör användas så att endast mottagaren kan komma åt informationen. DI:s rekommendation ”Hantera personuppgifter i e-post” . Ha interna riktlinjer!

Personuppgiftsansvaret - antagningskanslier

– PuA är den som, ensam eller tillsammans med annan, bestämmer över ändamål och medel för behandlingen av personuppgifter.

– Personuppgiftsansvaret följer normalt ansvaret för den uppgift som behandlingen av p-uppgifter ska stödja.

– Nämnden som är skolhuvudman är PuA för den behandling av personuppgifter som sker i dess verksamhet

– Den nämnd som har ett antagningskansli inom ramen för ett samverkansområde är PuA för den behandling som sker i kansliets verksamhet.

Vad kan hända?

– Beslut om att registret inte får föras

– Varning, reprimand, förelägganden

– Skadestånd till de registrerade (grupptalan)

– Höga administrativa sanktionsavgifter

– Dagsböter/fängelse? Inga straffbestämmelser i dataskyddslagen

– Skada på ”varumärket”

Vad har hänt efter 25/5 2018

- Datainspektionen är tillsynsmyndighet.
- Utdömda sanktionsavgifter?
- Hur rapporterar man incidentrapporter till Datainspektionen?
- Personuppgiftsbiträdesavtal, när krävs det?
- Dataskyddsombud skall finnas på plats.
- EU-gemensamma vägledningar finns i svensk översättning. Om bl a automatiserat beslutsfattande, anmälan av personuppgiftsincidenter , personuppgiftsbehandling som innebär hög risk och krav på konsekvensbedömning, samtycke , information till registrerade.

Ett urval ur SKL:s 10 informationsinsatser kring nya dataskyddsförordningen. (www.skl.se)

- Vad innebär dataskyddsförordningen? webbinar och PP-bilder. 18 maj 2016.
- Dataskyddsförordningen och dataskyddsombud. Webb-sändning och PM i PDF-format. 27 april 2017.
- Dataskyddsförordningen för beslutsfattare m fl. Vad måste göras före 25.5 2018 ? . Webb-sändning, november 2017.
- Skolan och dataskyddsförordningen, webbinar, 21 februari 2017.
- Vägledning , reglerna om dataskyddsombud i dataskyddsförordningen.
- PM, Checklista, annons, rekrytering av dataskyddsombud
- Mall och PM om registerförteckning. Mall, personuppgiftsbiträdesavtal (version 2.0 är på gång)