Dataskyddsförordningen
GDPR

När?

Dataskyddsförordningen 25 maj 2018.

Dataskyddslag - SOU 2017:39 En ny dataskyddslag – kompletterande bestämmelser till EU:s dataskyddsförordning.

Vad är en personuppgift?

All slags information som direkt eller indirekt kan hänföras till en fysisk person som är i livet. Typiska personuppgifter är personnummer, namn, telefonnummer, adress, ip-adresser och kontonummer. Även foton (där individ kan identifieras), videoupptagning och ljudinspelningar som lagras elektroniskt kan klassas som personuppgifter.

Känsliga personuppgifter
Ras/etniskt ursprung, politisk uppfattning, religiös eller filosofisk övertygelse, fackligt medlemskap, hälsa, genetik och biometri.

OBS! Normalt förbjudet att hantera känsliga personuppgifter men det finns undantag.

Behandling av personuppgift

Varje åtgärd eller serie av åtgärder som vidtas i fråga om personuppgifter till exempel insamling, registrering, organisering, lagring, bearbetning, ändring, återvinning, inhämtande, användning, utlämnande genom översändande, spridning eller annat tillhandahållande av uppgifter, sammanställning eller samkörning, blockering, utplåning eller förstöring.

Roller

Personuppgiftsansvarig, PuA
Den som ensam eller tillsammans med andra bestämmer ändamålen med och medlen för behandlingen av personuppgifter.

Personuppgiftsbiträde
Den som behandlar personuppgifter för den personuppgiftsansvariges räkning. Ex. outsourcat lönesystem.

Dataskyddssombud, DPO, DO
En fysisk person som, efter förordnande av den personuppgiftsansvarige, självständigt ska kontrollera att dataskyddsförordningen följs inom organisationen.
Frivilligt för företag om inte kärnverksamheten är att regelbundet, systematiskt och i stor omfattning övervaka enskilda personer eller att behandla känsliga personuppgifter eller uppgifter om brott i stor omfattning.

När får en personuppgift samlas in?

1. **Rättslig grund för behandling - i unionsrätt eller svensk rätt.**
   - Rättslig förpliktelse - skyldighet att registrera personuppgifter, ex uppfylla bokföringsskyldigheten i bokföringslagen.
   - Avtal - anställningsavtal, kundavtal och leverantörsavtal. (lönesystem, kundregister)
   - Samtycke - Be personen om att få registrera uppgifter om henne/honom. Krävs tydlig info om vilka uppgifter som samlas in och vad de ska användas till. (webbplats, vissa uppgifter i kundregister)
   - Intresseavvägning - Visa att företagets intresse av att hantera uppgifterna väger tyngre än den enskildes rätt till privatliv. (register med potentiella kunder, webbplats)

forts. när en personuppgift får samlas in.

2. Ändamålsbegränsning. Uttryckligt angivna och berättigade ändamål. Personuppgifterna får inte användas med annat syfte än vad de samlats in för.
3. Uppgiftsminimering. Endast uppgifter som är nödvändiga för ändamålet.
4. Korrekthet. om nödvändigt uppdaterade, åtgärder måste vidtas för att säkerställa att felaktigheter i förhållande till de ändamål de behandlas raderas/rättas utan dröjsmål.
5. Lagringsminimering. Inte förvara uppgifterna i en form som möjliggör identifiering längre än nödvändigt
6. Integritet och konfidentialitet. - Skydda personuppgifterna mot obehörig/otillåten behandling och mot förlust, förstöring/skada med lämpliga tekniska/organisatoriska åtgärder.

Ansvarsskyldighet - PuA ansvarar för och kunna visa att de sex principerna efterlevs.

Slopad missbruksregel

Missbruksregeln innebär att man idag kan använda enklare regler för personuppgifter i ostrukturerat material som t.ex. information om personer i e-post, på internet eller i en enkel lista som man har i datorn.

När missbruksregeln försvinner innebär det att samma regler som gäller för personuppgifter i databaser och ärendehanteringssystem, också ska användas för det som skrivs om personer i exempelvis e-post och på webbplatser. Det kommer att innebära krav på att bland annat ha en rättslig grund, informera de registrerade och föra register över sina behandlingar.

Långtgående informationskrav

Informationen ska innehålla följande men behöver inte ges om den registrerade redan känner till informationen:

A) Identitet och kontaktuppgifter för den PuA och för dennes företrädare samt eventuell DO.
B) Syftena med den behandling för vilken personuppgifterna är avsedda och den rättsliga grunden för behandlingen.
C) Hur länge uppgifterna kommer att lagras.
D) Om behandlingen är baserad på en intresseavvägning, PuA:s eller en tredje parts berättigade intressen.

forts. informationskrav

E) Mottagarna eller de kategorier av mottagare som ska ta del av personuppgifterna. I tillämpliga fall, att PuA avser att överföra personuppgifterna till en mottagare i ett tredjeland eller en internationell organisation.
F) Förekomsten av rättigheten att av PuA begära tillgång till och rättelse eller radering av de personuppgifter eller begränsning av behandling av personuppgifter som rör den registrerade och att invända mot behandlingen av sådana personuppgifter samt rätten till uppgiftsportabilitet.
G) Om behandlingen grundar sig på samtycke, rätten att dra tillbaka sitt samtycke när som helst, utan att detta påverkar lagligheten i behandling på grundval av samtycket innan detta drogs tillbaka.

H) Rätten att inge klagomål till Datainspektionen.

forts. informationskrav

I) Huruvida tillhandahållandet av personuppgifter är ett lagstadgat eller avtalsenligt krav, eller ett krav som är nödvändigt för att ingå ett avtal, samt huruvida den registrerade är skyldig att tillhandahålla uppgifterna och de möjliga följderna om sådana uppgifter inte lämnas.
J) Sådan förekomst av automatiskt beslutsfattande, inbegripet profilering och information rörande skälen, samt betydelsen och de förutsedda följderna av sådan profilering av den registrerade.
K) Om PuA avser att ytterligare behandla uppgifterna för ett annat syfte än det för vilket de insamlades ska PuA före denna ytterligare behandling ge den registrerade information om detta andra syfte.

Skyldighet att föra register över behandlingar

Elektroniskt register över företagets behandlingar

- Namn och kontaktuppgifter för företag
- Anledning till uppgiftsbehandling
- Beskrivning av kategorier av registrerade personer och personuppgifter
- Kategorier av organisationer som får uppgifterna
- Överföring av uppgifter till ett annat land eller annan organisation
- Tidsgräns för borttagning av uppgifter, om möjligt
- Beskrivning av säkerhetsåtgärder som används vid behandling, om möjligt

Företag med färre än 250 anställda behöver bara föra register om behandlingen

- är ett hot mot människors rättigheter och friheter,
- är regelbunden,
- eller gäller känsliga uppgifter eller beslastningsregister.

Registerutdrag

Den registrerade ska ha rätt att av PuA få bekräftelse på huruvida personuppgifter som rör honom eller henne håller på att behandlas och om sådana personuppgifter håller på att behandlas, tillgång till uppgifterna och följande information.

A) Ändamålen med behandlingen.
B) De kategorier av personuppgifter som behandlingen gäller.
C) De mottagare eller kategorier av mottagare till vilka personuppgifterna har lämnats eller ska lämnas ut, särskilt mottagare i tredjeländer eller internationella organisationer.
D) Om möjligt, den förutsedda period under vilken personuppgifterna kommer att lagras eller, om detta inte är möjligt, de kriterier som används för att fastställa denna period.

forts. registerutdrag

E) Förekomsten av rätten att av PuA begära rättelse eller radering av personuppgifterna eller begränsningar av behandlingen av de personuppgifter som rör den registrerade eller att invända mot behandlingen av sådana personuppgifter.
F) Rätten att inge klagomål till en tillsynsmyndighet.
G) Om personuppgifterna inte samlas in från den registrerade, all tillgänglig information om varifrån dessa uppgifter kommer.
H) Förekomsten av automatiserat beslutsfattande, inbegripet profilering.

Notifieringsskyldighet vid personuppgiftsincident

Vid personuppgiftsincident = skyldighet för personuppgiftsansvarig att inom 72 timmar från man fick reda på incidenten meddela Datainspektionen. I vissa fall även informera de registrerade.

Personuppgiftsincident = en säkerhetsincident som leder till oavsiktlig eller olaglig förstöring, förlust eller ändring av de personuppgifter som behandlas. Det kan också vara fråga om en personuppgiftsincident om en säkerhetsincident leder till obehörigt röjande av eller obehörig åtkomst till de behandlade personuppgifterna.

Dataportabilitet

En slags konsumenträttighet.

1, den registrerade har rätt att, när grunden för automatiserad behandling är samtycke eller avtal, få ut de personuppgifter som denne har tillhandahållit PuA i ett strukturerat, allmänt och maskinläsbart format och ha rätt att själv föra över uppgifterna till ny PuA.

2, Den registrerade har också rätt att begära få sina uppgifter överförda direkt från den PuA, när detta är tekniskt möjligt.

Privacy by design

Begreppet privacy by design = låta integritetsfrågor påverka systemets livscykel – från förstudie och kravställning via design och utveckling till användning och avveckling.

Datainspektionen

Datainspektionen ska utöva tillsyn.

Befogenheterna anges i dataskyddsförordningen.

En registrerad kan klaga till Datainspektionen.

Konsekvenser

Den registrerade har rätt till ersättning från den personuppgiftsansvarige eller ett biträde om skada har uppstått på grund av överträdelser av dataskyddsreglerna.

Datainspektionen kan besluta att ett företag som inte följer reglerna i förordningen ska betala en administrativ sanktionsavgift på upp till 20 miljoner euro eller fyra procent av den globala årsomsättningen.

Mer info

Datainspektionen
https://www.datainspektionen.se/dataskyddsreformen/

YouTube: sökord Dataskyddsförordning

Registerförteckning, SKL