GDPR

General Data Protection Regulation

EU:s nya dataskyddsförordning

Träder i kraft 2018-05-25

EUROPEISKA UNIONEN
Europeiska regionala utvecklingsfonden

Visit VÄRMLAND

Vad innebär den nya dataskyddsförordningen?

Dataskyddsförordningen kommer att påverka alla branscher, företag och organisationer som hanterar personuppgifter.

EU:s nya dataskyddsförordning General Data Protection Regulation, GDPR, som träder i kraft den 25.e maj 2018, innebär bland annat hårdare krav på hantering av personuppgifter. Det kommer att ställas krav på nya rutiner och processer för säker hantering av register samt krav på ansvarig ledningsnivå.

Nya dataskyddsförordningen kommer att gälla för alla organisationer och branscher som sparar eller på något sätt hanterar personlig och känslig information om sina anställda eller sina kunder.

EUROPEISKA UNIONEN
Europeiska regionala utvecklingsfonden

Visit VÄRMLAND

Vad är då en personuppgift?

Varje upplysning som avser en identifierad eller identifierbar person

”Identifierbar” = även indirekt information

Namn
Bankkonto
E-post
Vanor
Foton
Inlägg på sociala medier
Uppgifter om hälsa
Prenumerationer
Inköp

Personnummer
Utbildning
Platser
Användarnamn
Lösenord
Intressen
Livsstil
IP-adresser
”Känsliga uppgifter”

EUROPEISKA UNIONEN
Europeiska regionala utvecklingsfonden

Visit VÄRMLAND

Vad är ”behandling”

- Allt man gör med personuppgifter
- Spelar ingen roll om behandlingen är automatiserad eller inte

Insamling
Registrering
Organisering
Strukturering
Lagring

Läsning
Användning
Utlämning genom överföring
Spridning
Radering

Exempel på behandlingar

Grunddatabas för personalinformation
Löneadministration
Tidrapportering
Löne-/och utvecklingssamtal
Filmer/bilder/foton
Bonusmål
Lönerevision
Reseservice
Prestationsmätningar
Kameraövervakning (regleras av kameraövervakningslagen)
Kontroll över GPS och fordonsdatorer
Kontroll över personalens användning av IT och telefoni
Kompetensdatabaser/CV
Publicering av hemsida/intranätet
Ärendehanteringssystem med fritext
Kontaktinformation till kollegor (tel nr, e-post)

Pensionsuträkningar/utbetalningar
Semesterlistor
Behörighetskontrollsystem
Ekonomisystem
Avgångsorsaker
Facklig information
Turordningslistor
Utrustningsregister
Förmånsprogram
Intressekonflikter
Rehabiliteringsutredningar
Gruppliv- och pensionsavgifter
Sjukförsäkringar
Loggar
Anhörighetsregister
System som inte längre används

När är behandling av personuppgifter laglig?

Samtycke

Avtal

Rättsliga förpliktelser

Intresseavvägning

EUROPEISKA UNIONEN
Europeiska regionala utvecklingsfonden

Visit VÄRMLAND

Hur förbereder du dig?

Se vilka områden du behöver se över och anpassa

- Styrelsen och företagsledningen har ansvar för att bedöma och hantera de risker företaget är utsatt för.
- Du behöver dokumentera hur anställdas och privatkunders personuppgifter hanteras. Det innefattar vilken typ av information ni har tillgång till, vilka personer och funktioner som har tillgång till den samt i vilka system och databaser den faktiskt finns.
- Som ett första steg behöver ni kartlägga era rutiner för att identifiera var personuppgifter hanteras och vilka integritetsrisker som finns. Eventuellt kan nya rutiner behövas tas fram för att uppfylla kraven, och i vissa fall räcker det med justeringar. Ni behöver även se över avtalen med underleverantörer som sköter IT-driften.
- Göra en kartläggning över era IT-system och var personuppgifter lagras, hur de överförs till andra system, parter och till länder utanför EU-området. Ni behöver också se över om det finns nödvändiga rutiner för att kunna informera kunder och anställda om vilka uppgifter som lagras, samt snabbt och enkelt kunna korrigera eventuella felaktigheter samt radera uppgifter.

EUROPEISKA UNIONEN
Europeiska regionala utvecklingsfonden

Visit VÄRMLAND

Från kartläggning till incidenthantering

1. **Kartlägg:** Vilka personuppgifter hanterar du, hur och varför?
2. **Analysera:** Vilka är integritetsriskerna och vilken skada kan de orsaka?
3. **Rådfråga:** Vilka intressenter behöver du rådfråga?
4. **Designa:** Hur ska du bygga in integritetsskydd från början i dina processer?
5. **Dokumentera:** Hur ska du bevisa att du uppfyller kraven?
6. **Engagera:** Vilken information ska du ge till allmänheten och anställda, och behövs samtycken?
7. **Utmaning:** Hur ska du hantera incidenter, problem och klagomål?
8. **Tillse:** Hur ska du säkerställa kunders och anställdas rättigheter och tillsyn?
9. **Sanktioner:** Hur ska du klara de allvarligaste regulatoriska sanktionerna och skadeståndskrav?
10. **Utse dataskyddsombud/ansvarig och säkerställ att tid och budget avsätts snarast**

EUROPEISKA UNIONEN
Europeiska regionala utvecklingsfonden

Visit VÄRMLAND

Så här har vi startat processen på Visit Värmland

- Deltagit på Handelskammarens utbildning om GDPR
- Halvdag intern workshop
- Utsett dataskyddsansvarig
- Prenumererat på juristsajt under en gratisperiod
- Uppföljning av intern workshop
- Samtyckesavtal – medlemsföretag/personal/styrelse
- Deltagit i SKL:s utbildning i GDPR för kommunikatörer
- Processar policy
- Kontaktat IT-leverantörer vi använder oss av
- Börjat se över våra egna register; mejl, crm, excel, TURID, personalregister osv

EUROPEISKA UNIONEN
Europeiska regionala utvecklingsfonden

Visit VÄRMLAND