GDPR VAD INNEBÄR DET FÖR SWEBOATS MEDLEMMAR

STOCKHOLM 2018-01-29

CIOVEA

Maj 2018 träder EU förordningen GDPR i kraft som innebär utökade krav på bolag rörande hantering av personuppgifter

Ny lagstiftning

- En ny EU förordning träder i kraft i maj 2018 och blir därmed även svensk lag
- Bakgrunden är en anpassning av lagstiftningen till en mer digital ekonomi där mer personuppgifter samlas in och utbyts
- Förstärkning av enskildas **rättigheter** och tydliggörande av **ansvar** och **skyldigheter** för den som behandlar personuppgifter
- Skapa en enhetlig och icke fragmenterad lagstiftning inom EU

Risker

- För att säkerställa regelefterlevnad tunga **sanktionsavgifter** på på upp till 20 MEUR eller 4% av omsättningen
- Harmonisering av hur regelverket tolkas och sanktioner utdöms inom EU
- **Varumärkesrisken** minst lika viktig som risken för sanktioner & potentiellt större påverkan ekonomiskt
- Riskfaktorer : Kunder, medarbetare, leverantörer & myndigheter

Angreppsätt

- Arbetet behöver bedrivas både preventivt men även reaktivt för att få effektiva processer.
- Preventivt: Upprätta processer, policys och rutiner samt roller & ansvar samt erforderlig dokumentation
- Reaktivt: Kunna svara upp på eventuella kontroller samt registerutdrag etc.

För att säkerställa regelefterlevnad men även för att inte utsätta ert bolag för onödiga varumärkesrisker behövs ett såväl proaktivt som reaktivt arbetssätt i förhållande till personuppgifter

CioVea

Forskning visar att bolags bristande hantering av personuppgifter kan vara lika skadligt som barnarbete för varumärket

”Om det avslöjas något ofördelaktigt kring hur ett företag använt sina personuppgifter, eller låtit andra använda den, så reagerar människor väldigt stark.

Förtroendet för företaget sjunker lika mycket om människor tycker de använder deras personuppgifter fel som om företaget inte kontrollerar om deras underleverantörer använder sig av barnarbete.”

Källa: Intervju med Richard Wahlund Professor på Handelshögskolan i Computer Sweden

Vad är en personuppgift?

Personuppgift är information som **direkt** eller **indirekt** kan hänföras till en **levande person (ej juridisk person)**

Exempel på direkta eller indirekta personuppgifter:

- Namn, personnummer, adress
- Mobilnummer eller telefonnummer
- E-post adress
- Organisationsnummer (enskild firma då org.nummret är ett personnummer)
- Registreringsnummer för fordon, Chassinummer
- Kundnummer/ordernummer/fraktnummer
- Fastighetsbeteckning, lägenhetsnummer
- IP-nummer
- Foton, film, ljudupptagning
- **Etc……**

Vad är en känslig personuppgift och när får de behandlas

- Känsliga personuppgifter
  - Hälsouppgifter, provsvar etc.
  - Sexualliv och sexuell läggning
  - Ras- eller etniskt ursprung
  - Politiska åsikter
  - Religiös eller filosofisk övertygelse
  - Medlemskap i fackförening
  - Genetiska- och biometriska uppgifter

- Får endast behandlas med stöd av samtycke. Inom HR får de även behandlas om det krävs för att för att fullgöra skyldigheter inom arbetsrätten

Vad är en behandling?

Med **Behandling** avses tex:

- Insamling
- Registrering
- Lagring
- Utlämnande
- Överföring/Spridning
- Radering av personuppgifter

Gäller alla typer av registrerade dvs uppgifter om kunder, anställda, leverantörer eller andra förekommande privatpersoner!

Laglig grund

Lagliga grunder som kommer vara aktuella för er…….

- **Avtal**: Behandlingen är nödvändig för att fullgöra ett avtal i vilket den registrerade är part (tex anställningsförhållande, föra kundregister, fakturering,)
- **Samtycke**: Den registrerade har lämnat sitt samtycke (tex bakgrundskontroller)
- **Rättslig skyldighet**: Behandlingen är nödvändig för att fullgöra en rättslig förpliktelse som åvilar den personuppgiftsansvarige (t ex redovisning av sociala avgifter för anställda, bokföring)
- **Intresseavvägning**: Behandlingen är nödvändig för ändamål som rör den personuppgiftsansvariges eller en tredje parts berättigade intressen, om inte den registrerades intressen eller grundläggande rättigheter och friheter väger tyngre och kräver skydd av personuppgifter, särskilt när den registrerade är ett barn (anhörig information, marknadskommunikation, kameraövervakning)

Lagliga grunder som sannolikt inte kommer vara aktuella för er…….

- **Vitalt intresse:** Behandlingen är nödvändig för att skydda intressen som är av grundläggande betydelse för den registrerade eller för en annan fysisk person. (t ex för räddningstjänsten vid olycka)
- **Allmänt intresse:** Behandlingen är nödvändig för att utföra en uppgift av allmänt intresse eller som ett led i den personuppgiftsansvariges myndighetsutövning. (t ex kreditupplysningsverksamhet, arkivering, forskning)

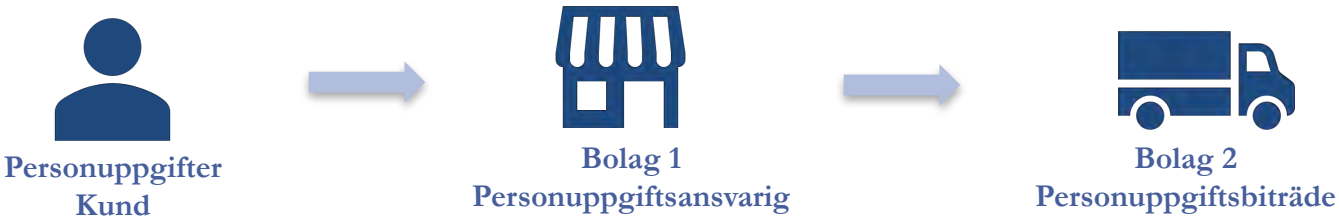
Ett praktiskt exempel på hur det kan tillämpas för er

Behandling	Syfte & ändamål	Laga stöd	Motivering	Behandlingstid
Administrera köp av tjänst eller produkt	Fullfölja avtal och leverera vara/tjänst till kund	Avtal	För att säkerställa att köpeavtalet hedras	1 år (för sällanköps varor kan det vara längre)
Lagring & arkivering	Upprätta bokföringsunderlag	Rättsligskyldighet	Bokföringslagen i Sverige kräver att underlag sparas i 7år	7 år
Spontan ansökning från kandidater	Spara och behandla spontan ansökningar som inkommer	Intresseavvägning	Diskrimineringslagen ger individen 2 år att åberopa diskriminering	2 år

Alla bolag har en laglig skyldighet att kunna uppvisa att man följer lagen och hur man har resonerat i de behandlingarna

Ni som bolag kan ha 2 ansvarsroller. Personuppgiftsansvarig eller Biträde

Exempel 1: Bolag 1 säljer en båt kund och anlitar Bolag 2 för att leverera båten till kunden.



Exempel 2: Bolag 1 ingår i en koncern och hanterar löneadministrationen åt ett annat bolag inom koncernen bolag 3

CIOVEA

Vad är en personuppgiftsansvarig?

- Den som bestämmer ändamålen med och medlen för behandlingen
- Juridiska personer - t ex SweBoat

Personuppgiftsansvariga är den som:

- som **samlar in personuppgifterna** från kund/medarbetare direkt eller indirekt
- bestämmer **från vilka** individer personuppgifter skall samlas in i från
- bestämmer **vilka personuppgifter** som skall samlas in
- **definierar lagligt** stöd för insamlingen
- **anger syftet** med insamlingen
- definierar **hur länge uppgifterna** skall **sparas**
- beslutar med **vilka uppgifterna** skall **delas**
- Självständigt **rätt** att **ändra**, **komplettera** eller **radera** uppgifterna

- Personuppgiftsansvaret kan delas med andra

Vad är ett biträde?

- Ett biträde är den som behandlar personuppgifter på uppdrag av den personuppgiftsansvarige:
  - Juridiska personer
  - t ex bolag som driftar system/databaser, fraktbolag, outsourcing
  - Biträdet är alltid en annan juridisk person kan dock vara inom koncernen
  - Biträdesavtal med instruktioner ska upprättas (en försäkring)

- Ett bolag kan både vara personuppgiftsansvarig och samtidigt agera biträde om vi behandlar uppgifter åt ett annan personuppgiftsansvarig.

- GDPR medför att biträdet får utökat ansvar och åläggas sanktionsavgifter om de inte följer lagstiftningen

Grundläggande principer - GDPR

Principer för behandling av personuppgifter

- **Laglighet, korrekthet och öppenhet** - det måste finnas en rättslig grund för behandlingen.
- **Ändamålsbegränsning** – ändamålen sätter ramarna för behandlingen, exv deltagarlistor
- **Uppgiftsminimering** - adekvata, relevanta och inte för omfattande i förhållande till de ändamål för vilka de behandlas.
- **Korrekthet** - korrekta och uppdaterade
- **Lagringsminimering** - inte sparas längre än nödvändigt, radera eller avidentifiera
- **Integritet och konfidentialitet** - skyddas mot obehörig eller otillåten behandling, mot förlust, förstöring eller skada
- **Ansvarsskyldighet** – kunna visa att principerna följs exv genom tydlig information, dokumentation, interna riktlinjer, utse DPO

Individensrättigheter – vad innebär det för er?

RÄTTEN TILL INFORMATION

- I samband med att individ lämnar ifrån sig personuppgifter ska de få information om hur uppgifterna hanteras
- Ska ske i samma media som insamling sker (tex till online, telefon, fysiskt)

RÄTTEN TILL TILLGÅNG

- Individ har rätt att ta del av all information om de personuppgifter som behandlas
- Kostnadsfri en kopia på de personuppgifter som är under behandling

RÄTTEN ATT RÄTTA

- Individ har rätt att rätta felaktiga uppgifter om sig själv eller komplettera uppgifter
- Rätten innebär dock inte att alla uppgifter **måste** rättas

RÄTTEN ATT RADERA/BLI GLÖMD

- Individ har rätt att bli radera/glömd om tex uppgifterna inte längre behövs för det ändamål de samlades in

RÄTTEN ATT INVÄNDA

- Individ har rätt att invända mot behandling
- Om personuppgifter används för marknadsföring har individen när som helst rätt att invända mot behandling och bolaget måste följa individens önskan

RÄTTEN TILL ATT BEGRÄNSA

- Rätt att begränsa behandling medans utredning föregår
- Tex vid identitetsstöld där kund bestrider uppgifterna korrekthet

RÄTTEN TILL PORTABILITET

- Rätt att få ut personuppgifter i ett maskinläsbart format

Vad behöver ni bolag ha på plats för att leva upp till lagen (minimum)

REGISTER & RÄTTIGHETSRUTINER

- Upprätta & dokumentera register
- Legitimt intresseanalys (LIA)
- Samtycken
- Designa & dokumentera rättighetsrutiner

FLÖDE AV PERSONUPPGIFTER & SÄKERTHET

- Kartläggning och dokumentation över flödet av personuppgifter internt & externt
- Säkertsåtgärder på data i vilja, i rörelse, i överföring
- Säkerhet (tex behörighet, loggar, back-up rutiner)

POLICIES & RUTINER

- Policies /rutiner som styr /stödjer de olika behandlingarna
- Intern integritetspolicy
- Konsekvensanalys (PIA) process & riktlinjer
- Incident rapporterings process & riktlinjer
- Test & utvecklingsrutiner för system

GALLRINGSRUTINER

- Definiera behandlings- & lagringstider
- Gallringsrutiner per behandling
- Rutiner för manuell radering /rättning av behandling

AVTAL & TREDJE LAND

- Biträdesavtal med era biträden eller då ni är biträden
- Dokumentation över behandlingar som sker utanför EU/EES
- Särskilda avtal om data behandlas i tredjeland dvs utanför EU/EES

ORGANISATION & KONTROLLER

- Dokumentation över roller & ansvar inkl DPO
- Årlig kontrollplan
- Utbildning för medarbetare & chefer

Kontaktuppgifter

Ylva Staszewski
email: ylva@ciovea.se
Tel: 070-360 5626

Henrik Johansson
email: henrik@ciovea.se
Tel: 073-263 63 10

APPENDIX

Nyckelförändringar i GDPR där anpassningar behöver göras för att uppfylla de nya kraven

Syfte & Laga stöd	• Dokumentation av syfte & rättsligt stöd i samband med informationsinhämtning

Registrerades rättigheter	• Den registrerade såväl kunder såsom medarbetare har följande rättigheter för vilka rutiner skall upprättas
	  • Information (alla kanaler)
	  • Bli glömd/raderad
	  • Invända registrering/profilering
	  • Tillgång - registerutdrag
	  • Rätten att flytta data /Portabilitet
	  • Rätta felaktigheter / begränsa behandling

Samtycken	• Särskilda och aktiva samtycken samt utökade dokumentations- & lagringskrav. PuA har bevisbördan
Incidenter	• Rutiner för att upptäcka och rapportera incidenter samt krav på dokumentation -72 timmars regeln
Konsekvensanalys (PIA)	• Krav på konsekvensanalys vid hantering av känsliga uppgifter eller där behandlingen kan skada eller försätta kunden i en oönskad situation
Privacy by design	• Arkitekturen är utformad och styr mot ett integritetssäkert användande i hela livscykeln från förstudie och kravställning via design och utveckling till användning och avveckling
Organisation	• Tillsättning av dataskyddsombud blir obligatoriskt för vissa verksamheter men kan vara till nytta för de flesta större verksamhet då ansvarsfördelning mellan styrelse och operativ verksamhet blir tydlig
Biträdesavtal	• Utökade krav på dokumentation och kontroll över personuppgifter som behandlas/överlämnas till leverantörers samt utökade krav på personuppgiftsbiträden
Säkerhet och accesskontroll	• Uppvisa säker lagring, överföring och radering av personuppgifter • Accesskontroller till data