Dataskyddsförordningen
Vad du som marknadsförare bör känna till

wednesday ACADEMY

SWEDMA

wednesday relations

Dataskyddsförordningen

Vad du som marknadsförare bör känna till

Axel Tandberg
SWEDMA
6 december 2016

Ett medlemskap som ger effekt | SWEDMA

Utveckling för marknadsföraren

Agenda

- Dataskyddsförordningen och personuppgiftslagen
- Innebörd för marknadsföringen
- Praktiska tips hur du anpassar dig till dataskyddsförordningen

SWEDMA

Bransch- och intresseorganisationen för direkt- och datadriven marknadsföring

- Påverkan
- Utbildning
- Inspiration
- Best practice

Personuppgiftslagen

Personsuppgiftslagen antogs i Sverige 1998
Baseras på dataskyddsdirektivet från 1995, ungefär samma grundnivå finns i hela den Inre Marknaden (dvs. EU + Norge, Island och Liechtenstein)

Syftet med lagen är att:

- Skydda den personliga integriteten
- Främja handeln med personuppgifter

Personuppgiftslagen gäller för all behandling av personuppgifter, oavsett om databasen i sig är B2C eller B2B

PuL – Roller

- Personuppgiftsansvarig:
  Den som bestämmer ändamålet med behandlingen (t.ex. Volvo)

- Personuppgiftsbiträde:
  Den som behandlar personuppgifter för annans räkning (t.ex. Volvos DM-byrå)

- Personuppgiftsombud:
  Person som förordnats av PU-ansvarig att utöva intern tillsyn

Dataskyddsförordningen

Dataskyddsförordningen publicerades i EUOT den 4 maj 2016
Kommer att ersätta PuL senast den 25 maj 2018

Anpassningen måste vara klar tills dess

Vad är skiljer DSF från PuL?
Det är en förordning, inte ett direktiv

Ny grundsyn

Grundstenen i förordningen är att ge INDIVIDEN rätten till informationen om denne, enligt Europakonventionen för de mänskliga rättigheternas 8e artikel.

Ett avgörande tillägg är organisationens ansvarsskyldighet (accountability) som medför bevisbörda för ATT och VARFÖR behandling skett

Personuppgift

Varje upplysning som avser en identifierad eller identifierbar fysisk person (nedan kallad en registrerad), varvid en identifierbarfysisk person är en person som direkt eller indirekt kan identifieras särskilt med hänvisning till en identifierare som ett namn, ett identifikationsnummer, en lokaliseringsuppgift eller onlineidentifikatorer eller *en eller flera faktorer som är specifika för den fysiska personens fysiska, fysiologiska, genetiska, psykiska, ekonomiska, kulturella eller sociala identitet.*

Behandling

Varje åtgärd som vidtas i fråga om personuppgifter – insamling, registrering, lagring, bearbetning, användning m.m.

PuL har ett undantag för ostrukturerad text, det försvinner med DSF

Dataskyddsombud

- Den nya benämningen av personuppgiftsombudet
- PuA och PuB måste ha ett DSO om
  - Myndighet alt. offentligt organ
  - Kärnverksamheten är behandling som övervakning
  - Kärnverksamheten är behandling av känsliga uppgifter
- Kontaktuppgifter ska offentliggöras och meddelas Datainspektionen

Utvidgat ansvar

- Enligt PuL är det endast PuA som är ansvarig för all behandling av personuppgifterna.
- DSF utvidgar detta ansvar:
  - PuA och PuB får delat ansvar för behandling
  - PuA måste ha kontroll på underleverantörers underleverantörer
  - Kunna visa att man tar ansvar genom att i förväg dokumentera vad man avser att göra

Nya principer för behandling

- Laglighet, korrekthet och transparens
- Ändamålsbegränsning
- Uppgiftsminimering
- Korrekta (personuppgifter)
- Lagringsminimering
- Integritet och konfidentialitet

Vad innebär detta i praktiken?

Som företagare måste man innan den 25 maj 2018 se över:

- Hur man samlar in uppgifterna/legal grund?
- Vilken information samlar organisationen in?
- Vem som har ansvaret för informationen?
- Vem som har tillgång och hur denne har tillgång till uppgifterna internt?
- Respektera individen!
- Om något händer?

Agera ansvarsfullt – dokumentera mera!

Insamling

I syfte att öka individens kontroll över sina uppgifters behandling så måste organisationerna informera individen om ett drygt dussin olika aspekter

- Detta måste göras på ett enkelt och lättbegripligt sätt. Speciellt om ni samlar in från barn
- Samtidigt skiljer man på när man samlar in själv eller använder tredje parts uppgifter

- Känsliga uppgifter (ex. hälsa) – kräver ett aktivt samtycke, se till att lägga till det.

Information vid insamling

Kort text som informerar om

- Personuppgiftsansvarig
- Syftet för bearbetning (dvs informera om verksamheten, riktad marknadsföring, profilering, etc...).
- Annan relevant information som alla mottagare av uppgifterna.
- Om att tillhandahålla personuppgifter är obligatorisk eller ej.
- Den registrerades rättigheter.
- Hur individen kommer i kontakt med dataskyddsombudet.
- Länk till fullständig information.

Information vid insamling

Full integritetspolicy – ska även innehålla

- Ytterligare information om den registrerades rätt till tillgång och rättelse samt kontaktväg för utnyttja denna rätt.
- Invändningar mot bearbetning i marknadsföringssyfte eller för profilering.
- Om det finns tvingande delar eller om det är frivilligt att dela med sig av uppgifterna.
- Ange vilken tredje man (specifika företag, organisation eller bransch) uppgifter kan komma att vidarebefordras till.
- Detaljerad information om behandling, ex. hur länge den avses att sparas.
- Legal grund för behandling.
- Rätten att återkalla ett samtycke.
- Berättiga intressen om ni hävdar Legitimt intresse som grund för behandling.
- Om uppgifterna ska lämna Inre Marknaden – på vilken legal grund (Privacy Shield?).
- Individens rätt att klaga till Datainspektionen.
- Kontaktuppgifter för den registeransvarige.

Fått personuppgifterna av annan

Man ska informera

- Inom en rimlig period, senast inom en månad
- Om PU ska användas för kommunikation, senast vid första kommunikationen
- Om PU ska lämnas ut till annan, senast när de lämnas ut första gången

Information vid första kontakt

Kort text som informerar om

- Vem du fick adressen från samt adress till denne
- Vem som är Personuppgiftsansvarig, dvs ditt företag
- Ändamålen för bearbetning (dvs informera om verksamheten, riktad marknadsföring, profilering, etc...)
- Vilka uppgifter som behandlas
- Annan relevant information som alla mottagare av uppgifterna
- Legal grund för behandling
- Den registrerades rättigheter
- Hur individen kommer i kontakt med DSOn
- Länk till fullständig information

Legal grund

Behandling är endast laglig om och i den mån som åtminstone ett av följande villkor är uppfyllt:

- **Samtycke**
- Fullgöra ett avtal
- Fullgöra en rättslig förpliktelse
- Skydda intressen som är av grundläggande betydelse för den registrerade eller för en annan fysisk person
- Utföra en uppgift av allmänt intresse eller myndighetsutövning.
- **Legitimt intresse** föreligger

Samtycke

- Kräver en aktiv handling, passivitet godtas inte – tänk kreativt!
- Bekräfta vad man har samtyckt till – använd kanalen!
- Spara samtycket – datum och text

Känsliga personuppgifter

Krävs aktivt samtycke för att få behandla

- Ras & etniskt ursprung
- Politiska åsikter
- Religiös & filosofisk övertygelse
- Fackföreningsmedlemskap
- Hälsa
- Sexualliv eller sexuell läggning
- Genetiska uppgifter
- Biometriska uppgifter för att identifiera individ

Legitimt intresse

Intresseavvägning

- När du får rekommendation av annan
- Påläsning av uppgifter för att genomföra profilering

- Kontrollera att du har rätt att använda dig av uppgifterna

Vilken information

- Bara de nödvändiga uppgifterna – NI måste kunna motivera
- Känslig information – samtycke och säkerhet (hantering, loggning och lagring)
- Måste ange hur länge man sparar – X månader efter kundförhållandet upphörde samt för andra lagkrav etc.
- Gallra!
- Viktigt att veta var ni lagrar informationen – får inte lämna Inre Marknaden utan speciella åtgärder

- Information insamlad före 25 maj 2018?

Personnummer

- Upp till varje medlemsstat att bestämma hur man vill ha det – troligen som vi har det idag
- Grundkrav samtycke
- Undantag – måste vara klart motiverat med hänsyn till
  - Ändamål eller
  - Identifiering eller
  - Annat beaktansvärt skäl

Ansvar

- Ansvaret för informationens korrekthet, lagring etc är den som avgör ändamålet – dvs. företaget.
- Ansvaret för behandling:
  - Informationsägaren ansvarar för den ”mjuka” delen
  - IT-ansvarig ansvarar för den ”hårda” delen
- Ansvar även för behandling hos underleverantör – dokumentera process och avtal!
- Dataskyddsombud, person som ser till att man gör rätt

Privacy by design

I ert arbete ingår det att införa så mycket skydd det går:

- Pseudonymisering
- Gallring (Tidsintervall)
- Tillgång för endast de som behöver (Tidsintervall)
- Endast de uppgifterna som behövs
- Exportering in i andra system?

Säkerhet

När man funderar på säkerheten och IT-systemen ska man beakta:

- Den senaste utvecklingen
- Genomförande kostnaderna och behandlings art
- Sammanhang och ändamål
- Risk för intrång i individens rättigheter

Säkerhet

- Sommar2016
- Sommar201&
- Sommar+”2016

Privacy by design och säkerhet

Innebörden av detta blir:

- IT system måste vara uppdaterade
- Fundera på om bättre att använda pseudonymisering
- Kunna återställa databasen efter incident
- Testa regelbundet de tekniska och organisatoriska säkerhetsåtgärderna
- Organisationen är ansvarig att anställda inte går för långt

Tillgång till uppgifter

- Uppdatera vem som har tillgång med jämna mellanrum
- Använd gärna inloggat läge med kontroll på vad som sker – personligt lösenord
- Annan part – måste anges att de finns
- Skicka uppgifter vidare – tänk på säkerhet, gärna krypterad e-post

Respekt!

- Uppdatera varsamt
  - Personnummer – informera att ni vill använda er av det!
  - Viktigt med korrekt adress
  - Adressätta – Ja om vi har sagt det
- Individens uppgifter
  - Portabilitet
- Registerutdrag

Portabilitet

En individs rätt att få sin uppgifter flyttade till en annan part.

- Ska göras i en strukturerad, allmänt använt och maskininläsbart format.
- Kan skickas direkt till ett annat företag om individen begär det.
- Dock ENDAST den informationen som individen själv har gett till organisationen.

Registerutdrag

En individ har rätt att få ta del av ta del en kopia av de uppgifter som behandlas och information om:

- Ändamålen
- Vilka kategorier av PU
- Ev mottagare internt och 3e land/Int. Org.
- Period som PU lagras
- Fritext
- Rätt till rättelse/radering/begränsning/invändning
- Rätten att klaga till Datainspektionen
- Adresskälla om uppgifterna inte kommer från individen

Något händer

Personuppgiftsincident – något händer med databasen

- Mindre incident, DSO registrerar
- Större incident, meddela DI inom 72 timmar
  - Intrångets art, kategorier av uppgifter samt antalet det berör
  - Konsekvenserna detta kan innebära
  - Åtgärder som ni har vidtagit/föreslagit att vidta, inklusive de som mildrar effekten
  - Kontaktuppgifter till DSO
- Fara för integritetsintrång – meddela individen de sista tre punkterna

Sanktionsavgifter

Varje dataskyddsmyndighet kan besluta om att begära in sanktionsavgifter på upp till 20 miljoner Euro eller 4% av företagets globala omsättning föregående år.

Avgörande är

- Vad man har gjort.
- Hur länge det har pågått.
- Antalet berörda individer.
- Vilken skada dessa individer har lidit.

Samma avgifter inom EU…

Vilka effekter får DSF för kommunikationen

Ställer större krav på att ni verkligen gör det ni säger att ni ska göra.

Reglerna som berör HUR vi kommunicerar med en privatperson (ex. marknadsföringslagen) har inte ändrats, bara behandlingen av dennes uppgifter.

Marknadsföringsrätt inom EU

EU-rätten innehåller ännu så länge inte någon enhetlig marknadsföringslag

Gemensamma regler finns sedan tidigare för vissa delar av marknadsföringsrätten, exempelvis vilseledande reklam och jämförande reklam

När enhetlig EU-rätt saknas gäller den nationella rätten i varje medlemsland med stora skillnader som följd

Marknadsföringsrätt inom EU

Förändringar på gång! Kommissionen vill ha en digital inre marknad senast 2018 – därför pågår det en översyn av allt som rör konsumenter och marknadsföring:

- Geoblocking
- e-Privacy direktivet
- Free flow of Data
- Internet of Things
- Etc.

E-post och SMS

- Kraven rörande ett aktivt samtycke återfinns i marknadsföringslagen
- Baserat på e-Privacy direktivet
- Kraven består därför.
- Viktigt att vara än tydligare när företaget samlar in e-postadress/ mobilnummer för att tillgodose ändamålskraven i DSF.

- Finns funderingar på att ändra, men vi vet inte hur.

TM

- Kraven återfinns i marknadsföringslagen, idag opt-out
- Baserat på e-Privacy direktivet
- Diskussioner om att införa ett aktivt samtycke
- Viktigt att vara en ansvarsfull aktör, följ de existerande etiska reglerna

Cookies

- Behandlingen av Cookies baseras även den på e-Privacy direktivet
- Implementerades i LEK
- Krav på samtycke som inte är passivt

- Finns långa diskussioner om att ta bort cookies och säga att de skyddas under DSF
- Samtidigt finns det krav på att stärka reglerna och se till att det blir aktivt samtycke – alla cookies samlar inte in personuppgifter

Men vad gör vi nu?

- ANDAS, gör yoga och acceptera att allt är föränderligt
- Det är inte helt klart än – den ska tolkas av 28 länders olika dataskyddsmyndigheter
- Engagera dig – påverka processen
- Kontrollera att ni lever upp till PuLs krav
- Kolla checklistan

Gör en översyn var ni är idag!

- Vilka personuppgifter behandlar organisation idag?
- Hur behandlar man dem?
- Har man inom organisationen dokumenterat processerna?
- Identifiera organisationens flöden.
- Vilka säkerhetsmekanismer har företaget, internt och externt?
- Vilket är organisationens skyldigheter – är ni PuA eller PuB?

Ändra synen på personuppgifter

- Ansvarsskyldigheten kommer att tvinga fram en ny syn på skyddet för personuppgifter
- Diskutera frågan i styrelsen redan idag
- Prata med en jurist
- Informera alla berörda delar av organisationen (ex. IT, kundsupport, kommunikationsavdelningen) att förändringar är på gång
- Leta reda på en bra DSO

Checklista:

- Se till att integritetspolicyn och handhavandet med personuppgifter är dokumenterad, uppdaterad och kommunicerad med anställda.
- Utbilda organisationens anställda
- Uppdatera organisationens IT-struktur och säkerhet, utveckla privacy by design.
- Gå igenom och anpassa alla avtal som berör personuppgiftsbehandling.
- PuA och PuB måste jobba mer som partners, båda är ansvariga för allt som görs – i ALLA led.

Tack för att ni lyssnade

Axel Tandberg

Jurist

SWEDMA

axel.tandberg@swedma.se

070 22 33 010