GDPR för e-handlaren

DET BEHÖVER DU VETA OM GDPR OM DU DRIVER EN WEBSHOP

En e-bok från Eseco System AB

Det behöver du veta om GDPR

Som e-handlare är det mycket man ska hålla koll på, inte minst vad gäller regelverk och lagar. Då försäljning på nätet automatiskt innebär hantering av kundernas personuppgifter är framförallt GDPR något man bör vara väl påläst om.

Men var börjar man? Vi har här samlat en praktisk e-bok som sammanställer det viktigaste, samt en översiktlig checklista för att ni ska kunna påbörja arbetet (eller fräscha upp minnet).

Trevlig läsning!

1. Vad är GDPR?

Vad är syftet med GDPR?

Dataskyddsförordningen, eller General Data Protection Regulation, är till för att stärka varje individs rättigheter genom att underlätta individens kontroll över sina egna personuppgifter. Målet är också att den enskilde ska få garantier om säker behandling av de egna personuppgifterna. GDPR gäller i hela EU för att bland annat skapa ett enhetligt skydd av personuppgifter utan att hindra det fria flödet inom EU och EES.

Dataskyddsförordningen är bara en av flera lagar och förordningar som handlar om dataskydd. Samtliga lagar grundar sig i de mänskliga rättigheterna och har skapats för att skydda alla individers integritet. På Integritetsskyddsmyndigheten kan du se hur lagarna hänger ihop.

Vad räknas som en personuppgift?

En personuppgift är information som kan leda till att identifiera en levande person. Det typiska man tänker på kanske är namn och adress, men det är även bilder och ljudupptagningar av individer, även om inga namn nämnts.

För att ge några exempel:

- Namn
- Adress
- E-postadresser som innehåller namn
- Personnummer
- ID-kortnummer
- Telefonnummer
- Foto på en person
- Ljudinspelning av en person
- Elektronisk data såsom IP-adress och cookies

Detta innebär att information som är kopplad till en juridisk person, exempelvis ett aktiebolag, inte är personuppgifter. Exempelvis organisationsnummer, e-postadresser såsom info@företag.se eller registreringsnummer på en firmabil. Rör det sig däremot om en enskild firma räknas det som en personuppgift, då det går att koppla till en fysisk person. Läs mer här om personuppgifter.

Vem får samla in personuppgifter?

De som behandlar personuppgifter är antingen en så kallad personuppgiftsansvarig eller ett personuppgiftsbiträde.

En personuppgiftsansvarig är den juridiska enhet (organisation/företag /stiftelse/myndighet) som samlar in och behandlar personuppgifter. Det är dennes ansvar att bestämma för vilka ändamål uppgifterna samlas in, behandlas och hur behandlingen ska gå till. Det betyder att det är ni som företag som är personuppgiftsansvariga.

Ett personuppgiftsbiträde är någon som behandlar personuppgifterna för den personuppgiftsansvarigas räkning. Det kan vara en fysisk eller juridisk person, offentlig myndighet, institution eller annat organ. Ex. vid kreditbedömning av kund eller vidarebefordran av personuppgifter till en distributör för fullgörande av avisering och leverans. Mellan personuppgiftsansvarig och personuppgiftsbiträde ska det finnas ett biträdesavtal.

2. Så påverkar GDPR e-handeln

Webshopen

De allra flesta e-handlare vill kunna analysera sin trafik på webshopen. För att göra det krävs elektronisk data från besökaren, främst deras IP-adress och data om hur de använder hemsidan. Detta kan göras genom att använda cookies och är viktigt att informera besökaren om. De ska kunna neka att datan samlas in under deras besök.

Använder ni en tredjepart såsom Google Analytics är det viktigt att dokumentera er insamling av datan. Vill ni läsa om hur Google hanterar cookies kan ni göra det här.

Ha även i åtanke om ni har information publicerad om era anställda på hemsidan, såsom bilder eller namn, så kräver även det dokumenterat samtycke från era medarbetare.

Orderhanteringen

Som e-handlare är det oundvikligt att behöva hantera kunders personuppgifter. Även om det är en självklarhet att kunden behöver lämna ut sina uppgifter om hen vill att ordern ska komma fram, krävs samtycke för att ni ska kunna få ta del av informationen. Tänk därför på att ha någon form av checkruta i checkouten där kunden ger sitt samtycke.

Viktigt att tänka på som e-handlare är att varje steg av insamling och behandling av personuppgifter måste dokumenteras var för sig. Det innebär att ni behöver separat dokumentering för såväl köp, betalning, reklamation, retur och byten av varor.

Marknadsföringen

Exempelvis om ni använder er av e-postmarknadsföring, kräver det insamling av personuppgifter i form av e-postadresser, namn, etc. Här är det viktigt att veta att ni inte kan ta vilka adresser som helst, utan för att skicka utskick krävs ett godkännande och samtycke från mottagaren. Det måste även alltid finnas en möjlighet för kunden att få sina personuppgifter raderade. Exempelvis via en avregistreringsknapp.

Lojalitetsprogram och medlemskap

Har ni ett lojalitetsprogram eller medlemskap för era kunder? Det kan vara ett bra sätt att samla in ytterligare information om era kunder, för att vidare kunna personalisera deras erbjudanden och helhetsupplevelse. Det blir även ett sätt att motivera insamlingen av mer data om individerna. Likt allt ovanstående kräver det dock en separat dokumentering av insamlingen.

På s.12 finns en smidig checklista för dokumentering av er personuppgifts-hantering.

3. Så säkerställer ni att ni följer GDPR

Bestäm ett dataskyddsombud på företaget

Dataskyddsombudets roll är att kontrollera att GDPR följs. För vissa företag är det obligatoriskt att ha ett dataskyddsombud. Det gäller företag som är något av följande:

1. Ett offentligt organ, såsom myndighet eller folkvald församling.

2. Om kärnverksamheten är att regelbundet, systematiskt och i stor omfattning övervaka enskilda personer.

3. Om kärnverksamheten är att behandla känsliga personuppgifter eller uppgifter om brott i stor omfattning.

Även om ni svarade nej på alla 3 frågor kan det vara bra att ändå ha en ansvarig person, även om ni inte måste. Då får den personen en överblick över er hantering av personuppgifter och kan lättare se om något behöver ses över.

Vill du läsa mer om dataskyddsombud kan du göra det här.

Kräv samtycke vid insamling av alla personuppgifter

Som nämnt ovan är samtycket en av de viktigaste delarna i GDPR. För att samtycket från besökaren eller kunden ska vara giltigt behöver det uppfylla vissa krav.

- Samtycket ska ges frivilligt
- Samtycket ska ges med en aktiv handling (det vill säga att man inte får lov att ha en för-i-kryssad ruta med samtycke eller att man ska behöva klicka på en knapp för att inte ge sitt samtycke)
- Individen ska förstå vad samtycket innebär
- Individen ska kunna återkalla sitt samtycke

Samla bara in relevanta personuppgifter

Ni får inte samla in vilka personuppgifter ni vill, hur ni vill. Det finns några grundläggande principer som ni som företag måste uppfylla för att ha rätt att samla in uppgifterna.

- Ni får bara samla in personuppgifter för specifika ändamål. Dessa ändamålen ska tydligt vara angivna och berättigade.
- Ni får inte behandla fler personuppgifter än vad som behövs för det angivna ändamålet.
- När personuppgifterna inte längre behövs ska ni radera dessa.
- Samtliga insamlade personuppgifter ska skyddas, det vill säga att ni aktivt måste se till att inte obehöriga får tillgång till dem.

Skapa en personuppgiftspolicy

För att underlätta ert arbete med GDPR rekommenderar vi att skapa en policy. Bestäm er för hur ni hanterar personuppgifter internt inom just er organisation enligt GDPR och dokumentera detta samt informera tydlig internt om det samma. Det är viktigt att alla inom organisationen har samma information och agerar på samma sätt.

Säkra upp hanteringen av uppgifterna genom att sätta en lösenordspolicy till alla program ni använder. Ha exempelvis nolltolerans för handskrivna lappar med lösenord som vem som helst kan läsa för att sedan logga in på era e-postkonto, affärssystem eller webbplattformar.
Teckna även biträdesavtal med alla era partners som har åtkomst till era kunders eller anställdas personuppgifter för behandling.

Har ni en tydlig policy blir ert kommande arbete i framtiden mycket enklare! Se även till att inkludera en rutin för hur ni arbetar. Exempelvis att en gång per år gå igenom om ni har onödiga uppgifter.

3. Checklistan för dokumentering

Vår rekommendation är att alltid se till att dokumentera era steg. Skriv ner löpande hur ni arbetar med GDPR och hanterar personuppgifter. På så vis har ni ett underlag i fall en granskning blir aktuell. Här är några punkter att skriva ner och spara:

- [ ] **Vilka av era program eller system samlar in personuppgifter?** Medlemsregister, löneprogram, affärssystem och e-postlistor är några exempel.

- [ ] **Vem har tillgång till personuppgifterna och varför?**

- [ ] **Varför samlar ni in och sparar uppgifterna?** Kan ni garantera att ni inte samlar in uppgifter som ni inte drar nytta av?

- [ ] **Hur länge sparas uppgifterna? Samt, hur garanterar ni att ni inte sparar dem längre än nödvändigt?** Exempelvis har ni en rutin för radering eller anonymisering av uppgifterna?

- [ ] **Hur ser ni till att rätt person har tillgång till uppgifterna och att inte obehöriga får tillgång till dem?**

ESECO SYSTEM AB
Jörgen Kocksgatan 4, 21120 Malmö
www.eseco.se