Vad är GDPR och vad betyder den för ditt företag?

Internet har drastiskt förändrat vårt sätt att kommunicera på och hur vi utför våra vardagssysslor. Idag sker allt digitalt. Vi skickar e-postmeddelanden, delar dokument, betalar räkningar och köper varor online och oftast genom att fylla i våra personuppgifter utan att tänka efter.

Har du någonsin stannat upp och reflekterat över hur mycket personuppgifter som finns lagrade om dig på internet? Och vad som händer med den informationen?

Det handlar om bankuppgifter, kontakter, adresser, inlägg i sociala medier, information om din IP-adress, samt vilka webbplatser du har besökt – allt lagras digitalt.

Företagen informerar dig om att de samlar in denna typ av information så att de kan ge dig bättre service, erbjuda dig mer anpassad och relevant kommunikation, allt för att ge dig en bättre kundupplevelse.

Men vad är det verkligen de använder dessa uppgifter till?

Det är den fråga som har ställts och besvarats i EU och är grunden till att en ny europeisk dataskyddsförordning vid namn **GDPR** (General Data Protection Regulation) träder i kraft i maj 2018. Denna förordning kommer att förändra sättet ditt företag samlar in, lagrar och använder personuppgifter på.

I den här informationen hjälper vi dig att förstå vad GDPR är, hur den kommer att påverka ditt företag och ger dig några praktiska tips om hur du kan börja förbereda dig inför GDPR redan idag.

Vi erbjuder också IT plattformar och program anpassade för GDPR med högsta säkerhetsklass! Ring oss gärna för ett kravlöst och förutsättningslöst möte med oss på Linford.

Vad är GDPR?

Den 25 maj 2018 träder den nya europeisk dataskyddsförordningen,”**The General Data Protection Regulation** (GDPR) i kraft. Förordningen kommer att implementeras i alla lokala personuppgiftslagar inom hela EU och EES-regionen. Den kommer att gälla alla företag som säljer till och lagrar personuppgifter om medborgare i Europa, inklusive företag på andra kontinenter. Det ger medborgarna i EU och EES större kontroll över sina personuppgifter och säkrar att informationen skyddas i hela Europa.

Enligt GDPR-direktivet är personuppgifter all information som är kopplad till en person såsom namn, foto, e-postadress, bankuppgifter, inlägg på sociala medier, platsinformation, medicinsk information och datorns IP-adress.

Det görs ingen skillnad mellan personuppgifter om individen i hans eller hennes privata, offentliga eller professionella roll – personen ses som en och samma individ oavsett roll. I en B2B-situation handlar dessutom allt om individer som interagerar och delar information med och om varandra. Kunder på B2B-marknader är så klart företag, men relationerna som hanterar de affärsmässiga relationerna är individer.

Enligt GDPR har individer bl.a. följande rättigheter när det gäller vilken information som samlas in om dem:

1. Varje behandling av personuppgifter måst ha en laglig grund

För att det ska vara tillåtet att behandla personuppgifter måste det alltid finnas ett stöd i dataskyddsförordningen, en så kallad laglig grund. En sådan laglig grund är samtycke från den registrerade.

2. Rätt till tillgång

Detta ger individen rätt att få tillgång till sina personuppgifter och få veta hur dessa kommer att användas av företaget efter att de har blivit insamlade. På begäran av en individ är företaget tvunget att gratis och i elektroniskt format tillhandahålla en kopia av personuppgifterna.

3. Rätten att bli bortglömd
Om individen inte längre är kund eller vill återkalla det samtycke som har gett företaget rätt att använda personuppgifterna, har individen under vissa förutsättningar rätt att få sin information raderad.

4. Rätten till dataportabilitet
Individen har rätt att överföra sina data från en tjänsteleverantör till en annan. Och detta måste ske i ett vanligt och maskinläsbart format.

5. Rätten att bli informerad
Rätten för individen att bli informerad omfattar i princip alla typer av insamling av personuppgifter som företagen gör.

6. Rätten att få information korrigerad
Detta garanterar att individen kan få sina uppgifter uppdaterade om dessa är inaktuella eller felaktiga.

7. Rätten att begränsa behandling
Individen kan under vissa förutsättningar begära att dess uppgifter inte behandlas. Uppgifterna finns kvar, men dess använding begränsas.

8. Rätten att invända
Detta inkluderar rätten att avbryta behandling av personuppgifterna i syfte att använda dem för direkt marknadsföring. Det finns inga undantag till denna regel och all eventuell behandling i marknadsföringssyfte måste avbrytas så snart företaget får denna begäran. På samma sätt måste individen meddelas denna rättighet tydligt och klart i början av all kommunikation.

9. Rätten att meddelas
Om det har förekommit ett dataintrång som omfattar en individs personuppgifter, har individen i vissa fall rätt att få vetskap om detta inom skälig tid efter det att personuppgiftsbrottet blev känt.

Konsekvenser för affärsverksamheten med GDPR

Denna nya dataskyddsförordning sätter individen i förarsätet medan det åligger företagen och organisationerna att säkerställa efterlevnaden av den.

I korthet gäller GDPR alla företag och organisationer etablerade i EU, oavsett om databehandlingen sker inom EU eller inte. Även organisationer utom EU kommer att omfattas av GDPR. Om ditt företag erbjuder varor och/eller tjänster till medborgare i EU, gäller GDPR även för ditt företag. Alla organisationer och företag som arbetar med personuppgifter bör utse ett dataskyddsombud som arbetar med GDPR internt, för att säkerställa att förordningen efterlevs.

De företag och organisationer som inte efterlever GDPR riskerar stora böter, upp till **4 % av den årliga totala globala omsättningen eller 20 miljoner euro**, beroende på vilken av summorna som blir störst.

Många tror att GDPR bara är en IT-fråga, men det långt ifrån fallet. Förordningen medför genomgripande konsekvenser för hela företaget, inklusive det sätt man hanterar sina marknadsförings- och försäljningsaktiviteter på.

GDPR:s påverkan på ditt kundengagemang

Villkoren för att erhålla samtycke är strängare enligt GDPR. Individen har rätten att återkalla samtycke när som helst och det måste ges separata samtycken för olika bearbetningsaktiviteter. Detta innebär att du måste kunna bevisa att individen har samtyckt till en viss åtgärd, till exempel att få ett nyhetsbrev. Det är inte tillåtet att förutsätta eller lägga till en ansvarsfriskrivning och det räcker inte att erbjuda möjligheten att tacka nej. (opt-out)

Detta medför många förändringar i hur företag hanterar sina marknadsförings- och försäljningsaktiviteter. Företagen måste se över sina interna processer, lösningar och olika formulär för att följa reglerna för lagring och hantering av persondata, samt att efterleva bästa praxis för e-postmarknadsföring. För att kunna registrera att man önskar motta kommunikation behöver den potentiella kunden fylla i ett formulär eller markera en kryssruta och därefter i ett ytterligare e-postmeddelande bekräfta att åtgärden är korrekt.

Organisationer måste kunna bevisa att samtycke har erhållits i de fall där en individ motsätter sig mottagandet av kommunikation. Detta betyder att all data som samlas in måste ha en verifikationsspårning som är tid stämplad samt rapportinformation som specificerar vad kontakten samtyckte till och hur.

Om du köper e-postlistor är det fortfarande du som är ansvarig för erhållandet av att få rätt samtyckesinformation, även om det är en leverantör eller outsourcad partner som har varit ansvarig för insamlingen av data.

I B2B-världen möter säljare potentiella kunder på mässor, de utbyter visitkort och när de kommer tillbaka till kontoret lägger de till kontakterna till företagets utskickslista. 2018 kommer detta ställa högre krav på företaget för att kunna registrera informationen. Företag bör även se över sättet att samla in information om kunder.

Förberedelser inför maj 2018

En nyckelkomponent i GDPR-lagstiftningen är inbyggt dataskydd (”privacy by design”).

Det inbyggda dataskyddet kräver att alla avdelningar på ett företag grundligt går igenom sina personupplysningar och hur de hanterar dessa. Det finns flera saker ett företag måste göra för att efterleva GDPR. Detta är endast de första inledande stegen för att komma igång:

1. Kartlägg företagets data

Kartlägg var alla personuppgifter inom hela företaget kommer ifrån och dokumentera vad ni gör med uppgifterna. Identifiera var uppgifterna lagras, vilka som har tillgång till dem och om det föreligger några risker för uppgifterna.

2. Fastställ vilken data ni behöver spara

Spara inte mer information än nödvändigt och radera uppgifter som inte används. Om ditt företag samlar in mycket uppgifter utan någon riktigt relevant ändamål, kan du inte spara dessa personuppgifter. GDPR innebär en mer disciplinerad hantering av personuppgifter.

Ställ dig själv följande frågor under upprensningsprocessen:

- Av vilken anledning arkiverar vi dessa uppgifter istället för att radera dem?
- Varför sparar vi alla dessa uppgifter?
- Vad försöker vi uppnå genom att samla in alla dessa kategorier av personlig information?
- Är det mer lönsamt att radera än att kryptera denna information?

3. Inför säkerhetsåtgärder

Utveckla och implementera åtgärder för att skydda infrastrukturen och för att förhindra dataintrång. Detta innebär införande av säkerhetsrutiner för att snabbt kunna agera och meddela individer och myndigheter om ett intrång sker.

Kontrollera även detta hos dina leverantörer. Outsourcing fritar dig inte från ansvar. Du måste kontrollera att även de har de rätta säkerhetsrutinerna på plats.

4. Granska er dokumentation

Du måste granska samtliga företags policyer och information samt säkerställa att de uppdateras eller skrivs om. Nya handlingar med information till registrerade behöver tas fram och nya biträdesavtal.

5. Etablera rutiner för hantering av personuppgifter

Som tidigare nämnts har individer fler grundläggande rättigheter i enlighet med GDPR.

Du måste etablera riktlinjer och rutiner för hur du hanterar var och en av dessa situationer.

Exempelvis:

1. Hur ser processen ut om en individ önskar och har rätt att få sina uppgifter raderade?
2. Hur säkerställer du att detta görs på alla plattformar och att uppgifterna verkligen raderas?

3. Om en individ önskar överföra sina uppgifter enligt reglerna om dataportabilitet, hur gör du detta?

4. Hur bekräftar du att personen som begärde att få sina uppgifter överförda verkligen är den person som han eller hon utger sig för att vara?

5. Hur ser kommunikationsplanen ut om ni skulle utsättas för ett dataintrång?

Slutsats

Data är en värdefull valuta i den digitala världen.

Samtidigt som GDPR skapar utmaningar och huvudbry för företaget, så skapar den även möjligheter.

Ett företag som visar att de värdesätter individens integritet (utöver dess lagstadgade skyldigheter), som är transparent kring hur de använder informationen, som utformar och implementerar nya och förbättrade metoder för hanteringen av kunders uppgifter under hela livscykeln bygger grunden för ett djupare förtroende och fler lojala kunder.

Vi på Linford hoppas denna information har gett er mer vital kunskap samt förberedelse inför 25 Maj 2018. För ytterligare information eller om ni behöver se över er IT i företaget kan vi erbjuda er flertalet funktionstjänster där vi aldrig tummar på er säkerhet!

www.linford.se