

Analys/Maria Nilsson

GDPR-guide:
Bli redo steg för steg

25 maj 2018 är det dags. Då införs GDPR. En ny dataskyddsförordning med nya krav och höga sanktionsavgifter för den som missköter sig. Vi går igenom de viktigaste nyheterna och hur ni förbereder er.

"DET FINNS FOG FÖR VISS ORO
– FÖRORDNINGEN ÄR BÅDE
OMFATTANDE OCH HÅRD"

» GDPR, General Data Protection Regulation, är på allas läppar. Inboxen svämmar över av inbjudningar till olika utbildningar om den kommande EU-förordningen som reglerar hur organisationer och företag får hantera personuppgifter. Och frågorna hopar sig.

Och det finns fog för viss oro – förordningen är både omfattande och hård. Dataskyddsförordningen, som den heter på svenska, kommer att gälla på samma sätt i alla EU:s medlemsstater och ersätter därmed personuppgiftslagen, PUL, i Sverige när den träder i kraft den 25 maj 2018.

Dessutom vill EU-kommissionen införa en ny e-integritetsförordning, ePrivacy Regulation, samtidigt som GDPR införs. Det nya förslaget, som kanske är mest känt som "Cookie-förordningen", innebär nya krav gällande elektronisk kommunikation och är tänkt att förtydliga GDPR digitalt. Det nya förslaget har dock fått mycket kritik, inte minst från mediebolag som är oroad över tanken att internetanvändare från och med maj nästa år endast ska behöva godkänna cookies en gång, direkt i webbläsaren. Mediebolagen befärar att de flesta därmed kommer att tacka nej till cookies, vilket skulle utgöra ett allvarligt hot mot beteendestyrd annonsering. Om förslaget hinner bli klart och införs tillsammans med GDPR nästa år är fortfarande oklart.



MARIA NILSSON

Senior digital strateg

Digital strateg och driver det egna konsultbolaget Credicon, Creative Digital Consulting. Tidigare chef för di.se, chef för digitala medier på Dagens Samhälle och redaktör, projektledare och reporter på E24.se och IDG.

**Medie
världen**
Premium

Stärkt integritet

Vad handlar då GDPR om?

Generellt innebär den nya förordningen att organisationer som behandlar personuppgifter åläggs ett större ansvar och utökade skyldigheter, medan de registrerades rättigheter förstärks.

Det som är i fokus är medborgarnas integritet; det ska bli tydligt att det är den registrerade som äger sina uppgifter – inte de företag och organisationer som hanterar dem. Dessutom finns en ambition att harmonisera reglerna inom EU för att underlätta handeln mellan staterna.

Det handlar inte så mycket om att förbjuda hantering av personuppgifter, mer om att organisationer som behandlar personuppgifter ska ha kontroll över sina register och sin behandling och kunna beskriva detta både för tillsynsmyndigheten och för dem som de har i sina register. Och den registrerade ska ha en rimlig chans att neka till hanteringen.

GDPR berör alla organisationer som hanterar personuppgifter om anställda och kunder. Inom organisationen kommer detta att påverka i stort sett alla. Alla anställda behöver vara medvetna om vilken policy företaget har för att hantera personuppgifter och avdelningar som IT, personal, ekonomi, marknad och kommunikation kommer att vara extra berörda.

Definitionen av vad som är en personuppgift är bred. All information som direkt eller indirekt kan kopplas till en fysisk person som är i livet räknas som en personuppgift. Alltså alla former av uppgifter som gör att man kan identifiera en person. Hit räknas till exempel bilder utan namn, ip-nummer, geografisk positionering och e-postadresser enligt modellen förnamn.efternamn@företag.se.

Viktigaste nyheterna

För att leva upp till de nya kraven kommer det att krävas en hel del resurser. Men även om det är lätt att se detta som endast ett krävande och dyrt byråkratiskt arbete finns det vinster att hämta. En uppdaterad och rensad kunddatabas och tydliga och rena kundrelationer ger en utmärkt utgångspunkt för att bedriva en effektiv kundbearbetning.

Hur blir då organisationen GDPR-redo? Här följer en sammanställning av de viktigaste nyheterna:



"DET SKA BLI TYDLIGT
ATT DET ÄR DEN
REGISTRERADE SOM
ÄGER SINA UPPGIFTER –
INTE DE FÖRETAG OCH
ORGANISATIONER SOM
HANTERAR DEM"

Informationsskyldighet

Det finns tydligt angivet i förordningen hur den som registrerats ska informeras av den som ansvarar för behandlingen av uppgifterna, den personuppgiftsansvariga. Information ska ges vid insamlingen av data, både när den registrerade själv lämnar uppgifterna och när uppgifterna kommer från någon annan, till exempel från ett köpt register. Den registrerade ska också själv kunna begära ut ett registerutdrag.

Uppgifterna som ska uppges vid varje tillfälle skiljer sig åt. När den registrerade själv lämnar sina uppgifter ska bland annat detta uppges:

- ✳ Kontaktuppgifter till personuppgiftsansvarig
- ✳ Dataskyddsombud (om sådant finns)
- ✳ Ändamål med behandlingen av personuppgifterna
- ✳ Rättslig grund för behandling av personuppgifterna
- ✳ Berättigat intresse vid intresseavvägning
- ✳ Om det finns andra mottagare av personuppgifterna
- ✳ Om det görs en tredjelandsoverföring
- ✳ Lagringstid
- ✳ Vilka rättigheter den registrerade har
- ✳ Information om rätten att dra tillbaka samtycke (om sådant finns)
- ✳ Information om rätten att lämna klagomål till tillsynsmyndigheten
- ✳ Behandling av personuppgifter enligt avtal eller lag
- ✳ Om det förekommer automatiserat beslutsfattande och profilering
- ✳ Behandling av personuppgifterna för annat ändamål

När uppgifterna kommer från någon annan än den registrerade behöver källan anges samt vilka kategorier av uppgifter som samlats in. När den registrerade ber om ett registerutdrag gäller en något mindre version av listan ovan.

Det är alltså många parametrar organisationen behöver ha kontroll över. Dessutom ska informationen som ges vara kortfattad och lättbegriplig, framför allt när informationen riktas till barn.

Tydligare rättigheter

Den registrerade har förutom rätt att få information kostnadsfritt, även rätt att:

- Få felaktiga personuppgifter rättade
- Få personuppgifter raderade, "rätten att bli glömd"
- Invända mot, eller begränsa, vissa former av personuppgiftshantering
- I vissa fall få de personuppgifter de själva lämnat flyttade till en annan organisation i ett allmänt använt och maskinläsbart format (så kallad dataportabilitet)

Det kan behövas en ID-kontroll vid osäkerhet om vem som begär ut uppgifterna.



Fakta om EU:s dataskyddsförordning

» Dataskyddsförordningen förhandlades fram av EU-parlamentet, EU:s ministerråd och EU-kommissionen den 15 december 2015.

EU-parlamentet antog förordningen den 14 april 2016 och den anslogs i EU:s officiella tidning den 25 maj 2016.

EU-förordningen börjar gälla den 25 maj 2018 i samtliga EU-länder.

Regeringens utredningsdirektiv om införandet av EU-förordningen hittar du här: https://www.riksdagen.se/sv/dokument-lagar/dokument/kommittedirektiv/dataskyddsforordningen_H4B115

Hos datainspektionen hittar ni både mer information och förordningen i sin helhet.

Kontroll över behandlingen

De allra flesta som hanterar personuppgifter kommer att behöva sätta upp ett register över hur de behandlar personuppgifter. Detta ska sedan göras tillgängligt för tillsynsmyndigheten, som i Sverige är Datainspektionen, vid förfrågan. I förordningen står det tydligt vad detta register ska innehålla.

Nytt är även att de organisationer som hanterar personuppgifter åt någon annan, så kallade personuppgiftsbiträden, är tvungna att föra register, om än något mindre omfattande.

Det krävs också ett formellt avtal som reglerar vad personuppgiftsbiträdet får göra med uppgifterna den hanterar åt den personuppgiftsansvariga. Och det vilar ett ansvar på personuppgiftsansvariga att välja personuppgiftsbiträden med omsorg.



För varje personuppgift man lagrar behöver man fastställa vilken rättslig grund hanteringen vilar på. Det gäller även de personuppgifter man redan har. De rättsliga grunder det oftast kommer att handla om är "samtycke", "avtal med den registrerade", "rättslig förpliktelse" och "intresseavvägning".

Om man baserar behandlingen på samtycke måste man kunna visa att ett samtycke har lämnats. Kan ni inte visa upp samtycket, måste det hämtas in igen.

I förordningen står att ett samtycke bör vara en frivillig, specifik, informerad och otvetydig viljeyttring. Det betyder till exempel att ett tyst samtycke, eller en på förhand ikryssad ruta på en webbplats, inte längre bör gälla. Inom EU pågår det ett arbete med att ta fram en vägledning gällande just samtycke.

Personuppgiftsbehandling baserat på avtal kan det vara tal om till exempel om kunden tecknat en prenumeration och uppgifterna krävs för fakturering.

Vissa uppgifter måste den personuppgiftsansvariga behandla för att det är en rättslig förpliktelse, till exempel kräver bokföringslagen att vissa uppgifter lagras.

I en del fall går det att basera sin behandling av personuppgifter på en intresseavvägning om den registrerade till exempel är kund hos den personuppgiftsansvariga och kan förvänta sig denna typ av behandling.

"FÖR VARJE PERSONUPPGIFT
MAN LAGRAR BEHÖVER
MAN FASTSTÄLLA VILKEN
RÄTTSLIG GRUND
HANTERINGEN VILAR PÅ"

Ökade säkerhetskrav

Det finns omfattande krav på att personuppgifterna ska behandlas säkert. Och det handlar både om teknisk och organisatorisk säkerhet.

Tekniskt sett handlar det om att brandväggar, antivirus, uppdaterad mjukvara, backuper, kryptering, åtkomstloggar och incidenthantering behöver ses över. Och när nya IT-system byggs, eller befintliga görs om, ska ett skydd för personuppgifter byggas in, vilket kallas "Privacy by design".

Organisatoriskt behöver man ha kontroll på vem som kommer åt uppgifterna, att det finns rutiner för hur man behandlar personuppgifter och man behöver även titta på den fysiska säkerheten såsom larm och lås.

Om man drabbas av ett intrång som innebär att personuppgifter till exempel förstörs, förloras, ändras eller blir åtkomliga för obehöriga ska detta dokumenteras och anmälas till tillsynsmyndigheten, helst inom 72 timmar om incidenten medför en risk för de registrerades rättigheter och friheter. Vid incidenter som medför en allvarlig risk för den registrerade, till exempel vid en ID-stöld, ska även den registrerade informeras.

Skärpta straff

Straffavgifterna kommer att vara kännbara. Tillsynsmyndigheten kan döma ut administrativa sanktionsavgifter i två olika nivåer.

Antingen 2 procent av den globala omsättningen, eller maximalt 10 miljoner Euro, eller 4 procent av den globala omsättningen, och maximalt 20 miljoner Euro, beroende på vilken typ av förseelse det handlar om.

"VID INCIDENTER SOM MEDFÖR EN ALLVARLIG RISK FÖR DEN REGISTRERADE, TILL EXEMPEL VID EN ID-STÖLD, SKA ÄVEN DEN REGISTRERADE INFORMERAS"





"HAR NI INTE SATT IGÅNG
ERT GDPR-ARBETE ÄR DET
HÖG TID ATT GÖRA DET NU"

Bli redo: steg för steg

Har ni inte satt igång ert GDPR-arbete är det hög tid att göra det nu. Det är en hel del som ska göras – och mycket handlar om att ni behöver få kontroll över vilka uppgifter ni har var, och vad ni gör med dem.

1. Utse ansvarig/ansvariga och tillsätt en arbetsgrupp

» Myndigheter och vissa organisationer är skyldiga att utse ett Dataskyddsombud, men även om det inte gäller er är det en god idé att utse en eller flera ansvariga för personuppgiftsbehandlingen. Dessutom behöver alla avdelningar som på något sätt hanterar personuppgifter vara med i processen.

2. Gör en inventering

» Sätt upp ett register över er behandling av personuppgifter. Detta krävs antingen när Datainspektionen begär att få se hur ni behandlar personuppgifter, eller när ni ska informera den registrerade om vilka uppgifter ni har. Det har börjat dyka upp verktyg för dokumentation på marknaden och märker ni att Excel-arket blir för tungjobbat kan det vara en god idé att investera i ett sådant.

3. Identifiera prio-områden

» Sannolik är några områden mer eftersatta än andra och viss behandling mer riskfylld. Hantering av till exempel särskilt integritetskänsliga uppgifter och uppgifter om barn kräver särskilda åtgärder.

4. Rensa

» Besluta om vilka uppgifter som ska bort, och vilka som ska fortsätta behandlas på vilken rättslig grund. Tänk på att lagra så lite som möjligt.

5. Se över säkerheten

» Gå igenom både er IT-säkerhet och den fysiska säkerheten. Och börja redan nu ta höjd för att nya IT-system ska byggas så att de stödjer organisationens arbete med att följa dataskyddsförordningen.

6. Ta fram en mall för incidentrapportering

» Om något skulle hända är det bra att ha rutinerna på plats. Ta fram en mall och se till att ansvarskedjan är klar.

7. Ta fram en generell extern personuppgiftspolicy

» Ni behöver ha ett dokument som beskriver hur ni hanterar personuppgifter generellt. Denna behövs till exempel när ni är skyldiga att informera den registrerade vid insamlingen av uppgifterna.

8. Ta fram en extern personuppgiftspolicy för varje enskilt fall

» För olika personuppgifter kan hanteringen skilja sig åt. Ni behöver komplettera er generella policy med texter som beskriver hur ni hanterar uppgifterna i varje enskilt fall för att kunna fullgöra kravet på informationsgivning.

9. Skriv avtal med alla personuppgiftsbiträden

» Även om ni redan har avtal med era personuppgiftsbiträden behöver de sannolikt skrivas om.

10. Konsultera en jurist

» När ni gjort er inventering och tagit fram era texter kan det vara lämpligt att låta en jurist titta på era bedömningar av rättslig grund, policyskrivningar samt personuppgiftsbiträdesavtal.



LÄS OCKSÅ:
"De fem viktigaste nyheterna i EU:s dataskyddsförordning"

11. Utred vilken tillsynsmyndighet ni lyder under

» Om ni har verksamhet i flera länder kan ni behöva bestämma vilken tillsynsmyndighet ni tillhör. Tanken är att en organisation bara ska behöva svara inför en tillsynsmyndighet. Det är dock alltid möjligt för medborgare i ett viss land att vända sig till det aktuella landets tillsynsmyndighet och klaga.

12. Ta fram en intern personuppgiftspolicy

» Ofta kan det handla om att ändra en hel kultur. Det behöver finnas tydliga policies för behandling och ansvarskedjor.

13. Se över anställningsavtalen

» Ni kan behöva skriva om avtalen så att den täcker all behandling av era anställdas personuppgifter.

14. Ta fram en strategi för kommunikation mot kund

» Vänd er uppdaterade policy till något positivt när ni kommunicerar med era kunder, och se till att ni har tänkt igenom vilken typ av information de ska få och vilka medgivanden ni behöver ta in – ni vill undvika att behöva göra om proceduren allt för ofta.

15. Tillämpa

» Inför GDPR i det dagliga arbetet och följ upp med regelbundna kontroller.

LÄS OCKSÅ:
**"Så påverkas
webbplatser
av EU:s nya
dataskydds-
förordning"**

En snabbanalys av juristen
Axel Tandberg.

Så jobbar mediehusen med GDPR

» Medievärlden Premium skickade ut en enkät till ett antal mediehus för att fråga hur de arbetar med nya dataskyddsförordningen. Här är svaren:

Andreas Aspegren, onlinechef på Aftonbladet

Hur länge har ni jobbat med GDPR?

"Aftonbladet och Schibsted har jobbat systematiskt med frågor om persondata och privacy under lång tid. Det specifika arbetet med att leva upp till de nya krav som ställs i och med GDPR inleddes för drygt ett år sedan."



Vilken del av organisationen har huvudansvaret?

"Samtliga delar av Aftonbladet som kommer i kontakt med persondata har ansvar för att säkerställa att vi följer lagen. Genomlysningen av vilka åtgärder som behöver vidtas drivs av en ansvarig utsedd av Aftonbladets ledning. Själva projektet involverar nyckelpersoner från affärsorganisationen och drivs med stöd av Schibsteds Legal-, Produkt- och Teknikorganisation."

Hur många jobbar med detta?

"Projektet har en kärna på 5–10 personer, men involverar i omgångar betydligt fler."

Har ni köpt in system för register- och dokumenthanteringen?

"Ja, vi har köpt in ett externt system för detta."

Vad är svårast?

"Påverkan på användarupplevelsen med de nya lagkraven samt behovet av tydlighet i kommunikationen kring komplicerade frågor. Innan nya branschstandarder för hur detta ska fungera är på plats har vi en stor pedagogisk uppgift gentemot våra användare."

Ser ni några fördelar eller möjligheter i arbetet?

"Tydliga regler för vad som gäller gynnar hela branschen. Aftonbladet har ett högt förtroende hos såväl användare som annonsörer, något som kommer att bli ännu mer värt i framtiden."

Lennart Foss, vd för NTM

Hur länge har ni jobbat med GDPR?

"NTM-koncernen påbörjade aktivt arbete innan sommaren, men har varit medvetna om den nya förordningen länge och tagit den i beaktning. Vi har till exempel investerat i ny IT-miljö under våren 2017 och säkerställt hårdvara både för drift och den enskilda medarbetaren."



Vilken del av organisationen har huvudansvaret?

"NTM har tillsatt en projektledare som sköter planering och samordning ihop med en styrgrupp där personer från olika avdelningar inom koncernen; IT, utvecklingsbolag, HR, ekonomi och koncernledningsrepresentant ingår."

En förstudie av våra system och rutiner pågår, och ett antal projekt har påbörjats för att säkerställa att vi följer den nya dataskyddsförordningen."

Hur många jobbar med detta?

"En övergripande projektgrupp har tillsatts vilken sköter planering och tidplan. Åtgärd inleddes med systeminventering ur GDPR-perspektiv parallellt med att information om den nya förordningen förs ut i organisationen. De mest kritiska systemen är identifierade och åtgärdsplan igång. Varje system hos oss har en systemansvarig/produktansvarig, vilka är ansvariga att säkerställa att man följer GDPR. För de internt utvecklade systemen sker åtgärder ihop med pågående utvecklingsprojekt, för andra system sker säkerställandet tillsammans med respektive leverantör. Systemansvarig rapporterar till dataskyddsombudet på koncernnivå. Förutom att dokumentera och säkra alla system så behövs det mycket nya rutiner för hanteringen av personuppgifter. Så ja, det är många personer inblandade."

Har ni köpt in system för register- och dokumenthanteringen?

"Det pågår just nu en utredning kring hur behovet ser ut. Än så länge är det inte ett identifierat behov."

Vad är svårast?

"Mängden system vi har."

Ser ni några fördelar eller möjligheter i arbetet?

"Det är alltid bra att jobba med kvalitetsarbete, vilket detta faktiskt är."

Aller Media, Jenny Olsson, marknadschef.

Hur länge har ni jobbat med GDPR?

"Vi har hållit oss informerade under de senaste 2 åren och aktivt arbetat på vår egen anpassning sedan i våras."

Vilken del av organisationen har huvudansvaret?

"Huvudansvaret ligger inom vår kommersiella organisation. Det är där vi har mest data som behöver säkerställas."

Hur många jobbar med detta?

"Det är 5 personer som har huvudsakliga ansvar för olika områden både från business och IT. Många fler är dock involverade för att kunna genomföra förändringarna och säkerställa att vi blir compliant både för B2C, B2B, HR, IT system, leverantörsavtal och så vidare."

Har ni köpt in system för register- och dokumenthanteringen?

"Vi har Draftit sedan tidigare så vi har inte köpt in något nytt system."

Vad är svårast?

"Det är ett brett område som spänner över mer eller mindre alla delar av vår verksamhet och skapar därmed komplexitet. Det andra är möjligen att lagen är ny och det finns inte branschpraxis och tolkningar gjorda på den ännu."



Ser ni några fördelar eller möjligheter i arbetet?

"Det är en möjlighet att sätta resurser på området och säkerställa att all kunddata hanteras korrekt."

Bengt Salomonsson, IT-chef på Sörmlands Media:

Hur länge har ni jobbat med GDPR?

"Projektet startades i maj 2017."

Vilken del av organisationen har huvudansvaret?

"IT-avdelningen."

Hur många jobbar med detta?

"3 personer."

Har ni köpt in system för register- och dokumenthanteringen?

"Nej – inte i nuläget, vi använder befintliga dokumenteringssystem."

Vad är svårast?

"Svårt att peka på någon speciell punkt – mer än att det är omfattande."

Ser ni några fördelar eller möjligheter i arbetet?

"Även om det är omfattande så är det bra med en fullständig revision, genomlysning och uppdatering av våra system, processor, rutiner, avtal, etcetera. Samt att motsvarande även utförs av våra externa leverantörer. Rätt kommunicerat gentemot våra kunder kommer personuppgiftshanteringen att uppfattas som något positivt."



Mats Tidstrand, vd för Hallpressen

Hur länge har ni jobbat med GDPR?

"Sedan våren 2017."

Vilken del av organisationen har huvudansvaret?

"COO."

Hur många jobbar med detta?

"4 medarbetare."

Har ni köpt in system för register- och dokumenthanteringen?

"Upphandling pågår genom koncernens IT-bolag."

Vad är svårast?

"1. Hitta en struktur hur vi får fram rätt data på personnivå.
2. Hur ser eventuella undantag ut kopplat till media/journalistik och hur påverkas eventuellt källskyddet i samband med GDPR. Vilka är gränsdragningarna?"

Ser ni några fördelar eller möjligheter i arbetet?

En uppdatering/registrering av den samlade information som finns i företaget."

