:Datakollen

Kom igång med GDPR-arbetet!

1 Få koll på företagets personuppgifter

För att följa det nya regelverket behöver du först kartlägga:

- vilka personuppgifter som ni hanterar och
- om de klassas som känsliga eller inte:

Personuppgifter är t.ex. namn, adresser, telefonnummer och bilder.
Känsliga personuppgifter är t.ex. personnummer och bilder.

2 Meddela hur och varför du samlar in personuppgifter

Du behöver meddela kunderna/medlemmarna:

- **Hur** uppgifterna samlas in
- **Varför** uppgifterna behandlas
- **Hur länge** du planerar att spara uppgifterna. Och du får inte lagra dem längre än nödvändigt.

3 Ta fram en integritetspolicy

Integritetspolicyn bygger på uppgifter som tas fram i steg 1 och 2. Dessutom ska den bland annat innehålla:

- en hänvisning till GDPR
- den registrerades rättigheter
- hur personuppgifter överförs till tredje part

4 Upprätta rutiner för att radera personuppgifter

Rätten att bli bortglömd är en av nyckelprinciperna i GDPR. Det innebär att du måste kunna radera personuppgifter från och med den 25 maj. Mer specifikt måste du radera personuppgifter om:

- personuppgifterna inte längre behövs i förhållande till ändamålet de ursprungligen samlades in för
- den registrerade återkallar sitt samtycke till behandling (och det inte finns orsak eller berättigat intresse till att fortsätta behandla uppgifterna)
- personuppgifter har behandlats på ett otillåtet sätt

5 Hämta in samtycke till att samla in uppgifter

Om den lagliga grunden för en personuppgiftssamling är **samtycke** måste du kunna visa att de registrerade har lämnat sitt samtycke till hanteringen av deras personuppgifter.

Enligt GDPR måste samtycke till insamling av personuppgifter **ges fritt** och ska vara **specifikt**, **informerat** och **otvetydigt**. Samtycke kan inte ges implicit genom tystnad, förkryssade rutor eller inaktivitet. Du måste även informera de registrerade om rättigheten att bli bortglömd och tillhandahålla enkla sätt att återkalla samtycket på.

Samtycke är även en viktig faktor för företagets eventuella e-postmeddelanden. För kampanjerbjudanden, rabatter och annan kommersiell e-post till personer som inte är kunder måste du använda specifika alternativ för att de ska bekräfta sin prenumeration. Du får inte skicka kommersiell e-post till personer som inte lämnat uttryckligt samtycke.

För icke-kommersiell e-post (t.ex. hälsningar vid högtider) eller e-post till kunder krävs bara en möjlighet att avanmäla sig från sådan e-post.

Med andra ord: **uppdatera befintliga metoder** och se till att företaget uppfyller de nya GDPR-reglerna.

6 Utbilda alla medarbetare

Organisera **interna utbildningstillfällen** för att diskutera och förstå hur GDPR påverkar företaget. Arbetet med att göra medarbetarna medvetna om GDPR bör vara en kontinuerlig process med återkommande och dokumenterade diskussioner.

Kom ihåg att uppdatera interna dokument och rutiner som:

- policy för bärbara datorer
- e-post
- sociala medier
- anställningsavtal

7 Visa att företaget efterlever GDPR

GDPR-förordningen kräver att du kan intyga att du följer reglerna:

- dokumentera rutiner
- uppdatera integritetspolicy
- identifiera den lagliga grunden för behandlingen
- upprätta användarvillkor, kundavtal och databehandlingsavtal om du anlitar personuppgiftsbiträden och/eller underbiträden.

8 Upprätta avtal med samarbetspartners

Ett personuppgiftsbiträde är någon som behandlar data på uppdrag av den personuppgiftsansvariga och som inte är anställd i organisationen. Exempel på detta är företag som hanterar löneutbetalningar, revisorer och företag som gör marknadsundersökningar eller sköter IT-drift. Molntjänstleverantörer är i allmänhet också personuppgiftsbiträden. Se till att skriva personuppgiftsbiträdesavtal med de samarbetspartners som du delar ut personuppgifter till.

9 Skapa en krishanteringsplan

Alla företag behöver ha en **plan för incidenter**. Om en incident inträffar måste du i vissa fall rapportera det till Datainspektionen, ibland även till de berörda individerna. Det innebär att ni inte har tid att fundera ut vad som ska göras när ett intrång väl har inträffat, utan ni behöver ha rutiner på plats för att undvika böter.

När ni förbereder er inför den nya förordningen bör ni upprätta rutiner för att upptäcka, rapportera och undersöka sådana incidenter. Se till att alla på företaget förstår vad en personuppgiftsincident är, och att ni upptäcker varningssignalerna i tid.

10 Hantera åtkomstrutiner

Personer vars uppgifter företaget hanterar ska ha

- Rätt till **åtkomst** till alla sina personuppgifter
- Rätt att **korrigera felaktigheter**
- Rätt att **göra invändningar mot behandling** i vissa fall eller radera sina uppgifter.

Allt ska åtgärdas inom 30 dagar!

Om ni får många frågor om åtkomst bör ni överväga att utveckla metoder för att hantera ärendena på ett effektivare sätt. Kolla upp om ni behöver utveckla ett system där enskilda kan få åtkomst till sina uppgifter online. Detta rekommenderas av GDPR-myndigheterna i de flesta länder.

11 Dataskydd för minderåriga

Genom GDPR införs ett särskilt skydd för barns personuppgifter. Enligt GDPR kan **barn under 16 år inte ge juridiskt giltigt samtycke** eftersom de ”kan vara mindre medvetna om berörda risker, följder och skyddsåtgärder” kring delning av personuppgifter. Om ert företag tillhandahåller onlinetjänster till barn och ni förlitar er på deras samtycke till insamling av deras information behövs nu dessutom **samtycke från en förälder eller vårdnadshavare**.

12 Dataskyddsombud

Ni kan behöva utse ett dataskyddsombud som övervakar strategin och efterlevnaden av GDPR på företaget. Det här är inte obligatoriskt för de flesta små och medelstora företag, men Datainspektionen rekommenderar att alla företag utser ett ombud.

Du behöver inte anställa någon på heltid – dataskyddsombudet kan vara en extern konsult eller en medarbetare som tar på sig extra ansvar utöver sina dagliga arbetsuppgifter. Men se till att personen har goda kunskaper, stöd och kontakt med företagets högsta ledning för att bli effektiv i rollen som dataskyddsombud.

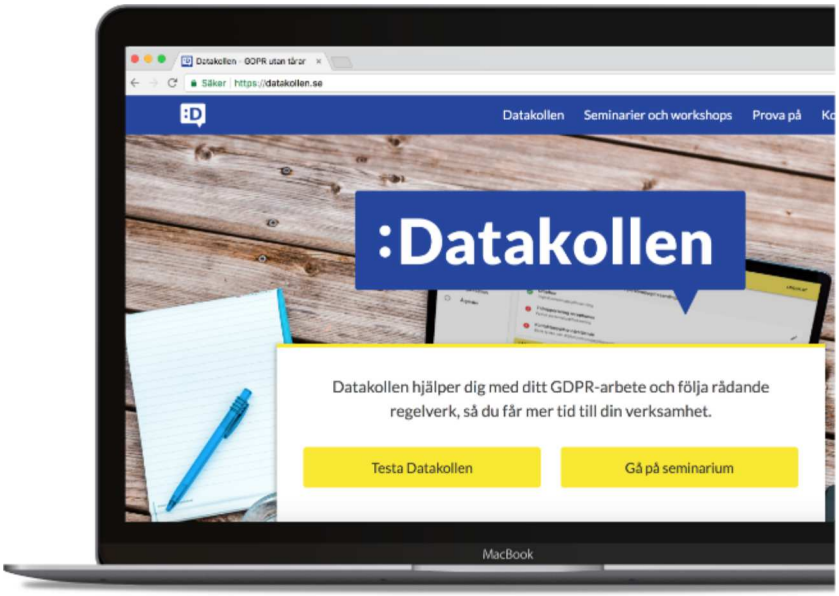
Specifika behov, eller vill du veta mer?

- Hör av dig!

stefan@datakollen.se

Stefan Johansson

Jurist och försäljningschef på Datakollen



Kom igång redan idag!

Skapa ett konto i Datakollen och kom igång med företagets GDPR-arbete redan idag!

Skapa ett konto

Lär dig mer om GDPR!

Nyfiken på hur GDPR påverkar ditt företag och hur du bör arbeta med den nya dataskyddsförordningen?

- Läs våra Frågor & Svar

Frågor & Svar