HANDBOK *GDPR*

företag*arna*

Innehåll

1. MÅSTE JAG ANPASSA MIG TILL GDPR?

Denna text är tänkt som en översiktlig introduktion till hur ditt företag ska hantera personuppgifter för att följa lagregler m.m.. Du hittar mer utförlig information på t.ex. Datainspektionens hemsida.

GDPR är en förkortning för EUs allmänna dataskyddsförordning som handlar om hur personuppgifter får hanteras i bl.a. företag. GDPR ger personer som befinner sig inom EU/EES skydd för hur deras personuppgifter kan hanteras av andra när det inte är en ren privat hantering. Det innebär att företag, myndigheter och organisationer måste ta hänsyn till GDPR när de ska behandla personuppgifter om t.ex. kunder, anställda och kontaktpersoner hos leverantörer.

Personuppgifter är alla uppgifter som direkt eller indirekt kan identifiera en fysisk person. Det är med andra ord inte bara namn och personnummer som omfattas av begreppet, utan även bilder, e-postadresser och mobiltelefonnummer kan omfattas. Ibland kan flera uppgifter tillsammans identifiera en person och då sammantaget bli personuppgifter.

1. MÅSTE JAG ANPASSA MIG TILL GDPR? forts.

Det är endast behandling av personuppgifter med automatisk databehandling och även annan behandling av personuppgifter som ingår i ett systematiskt register som omfattas av reglerna. Detta innebär att alla personuppgifter som t.ex. förvaras i dator, molnet eller mobiltelefon omfattas. Ett pappersdokument i sig självt utgör inte ett systematiskt register, men däremot exempelvis två pärmar med innehållsregister som hänvisar till varandra kan utgöra ett systematiskt register och behandlingen ska då omfattas av reglerna.

Detta innebär sammantaget att de allra flesta företag i Europa blir tvungna att följa och anpassa sig till reglerna i GDPR.

2. GDPR I SVERIGE

Datainspektionen är tillsynsmyndighet i Sverige och samarbetar med tillsynsmyndigheter i andra EU-länder och EDPB som är den europeiska dataskyddstyrelsen.

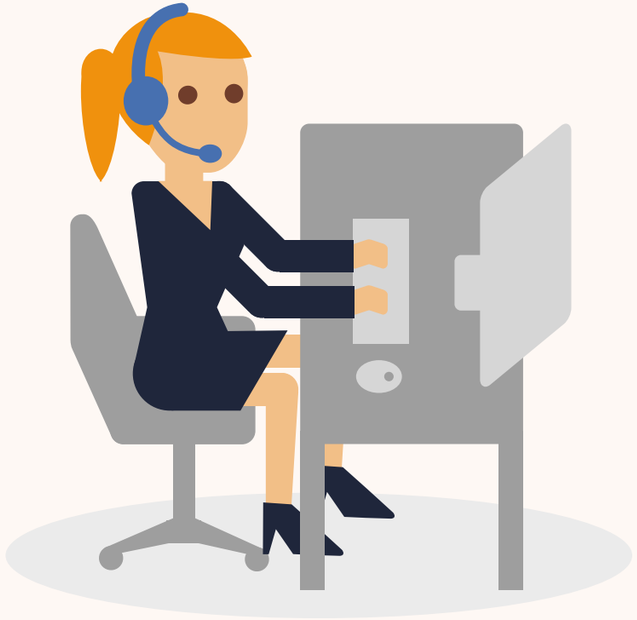
Varje land har en egen nationell lagstiftning som kompletterar GDPR. GDPR har dock företräde framför svensk nationell lagstiftning. Denna text tar upp vad som gäller i Sverige både enligt GDPR och svensk kompletterande lagstiftning.

Tillämpningen av GDPR får inte strida mot tryckfrihetsförordningen eller yttrandefrihetsgrundlagen. Det innebär att de som har utgivningsbevis för sin tidning eller webbplats har möjlighet att t.ex. hantera personuppgifter utan att informera de registrerade m.m.

Dessutom har Sverige utnyttjat möjligheten att undanta behandling av personuppgifter som sker för journalistiska ändamål eller för akademiskt, konstnärligt eller litterärt skapande från tillämpning av artiklarna 5–30 och 35–50 i GDPR och vissa delar av den kompletterande lagstiftningen. Detta innebär att i de fall då ditt företag behandlar personuppgifter för dessa ändamål behöver ditt företag bara följa reglerna om samarbete med tillsynsmyndigheten, säkerhet för behandlingen av personuppgifter och anmälan och information om personuppgiftsincident.

3. PERSONUPPGIFTSANSVARIG

Personuppgiftsansvariga är de som hanterar personuppgifterna för sina egna syften och ändamål. En personuppgiftsansvarig kan lämna över hanteringen till ett personuppgiftsbiträde som då behandlar personuppgifterna enligt den personuppgiftsansvariges instruktioner och syfte. Det är t.ex. ditt företag som är personuppgiftsansvarig för behandling av dina kunders personuppgifter för ändamålet att kunna fakturera. Har ditt företag lämnat över ansvaret för fakturering till en konsult av något slag, är det fortfarande ditt företag som är personansvarigt, eftersom det är ditt företag som har bestämt syftet med behandlingen. Däremot kan konsulten agera som ett personuppgiftsbiträde.



4. PERSONUPPGIFTSBITRÄDE

Ditt företag kan ge instruktioner till ett annat företag att behandla personuppgifterna för ditt företags ändamål och enligt ditt företags instruktioner. Det andra företaget är då ditt företags personuppgiftsbiträde. Mellan er ska då skrivas ett personuppgiftsbiträdesavtal som ska innehålla vissa punkter.

Du hittar en enkel mall för personuppgiftsbiträdesavtal på foretagarna.se

5.PRINCIPER FÖR BEHANDLING AV PERSONUPPGIFTER

För behandling av personuppgifter gäller följande principer

- laglighet och öppenhet
- ändamålsbegränsning
- uppgiftsminimering
- korrekthet
- lagringsminimering
- integritet och konfidentialitet

Detta innebär att du i din verksamhet bara får behandla personuppgifter som du har rättslig grund för att behandla, och inom de regler som finns (laglighet). Hen vars personuppgifter du behandlar ska få information om behandlingen (öppenhet). Du får bara behandla personuppgifterna för ändamål som är förenliga med det ändamål som de samlades in för, eller samtycke inhämtats till annan användning eller med stöd av rättsregler som är nödvändiga och proportionella i ett demokratiskt samhälle (ändamålsbegränsning). Dessutom får du inte behandla fler uppgifter i verksamheten än som behövs för ändamålet och inte lagra uppgifterna längre än de behövs (uppgiftsminimering). Det är ditt företags ansvar att personuppgifterna är korrekta och uppdaterade (korrekthet). Ditt företag ska också se till att behandlingen är säker så att uppgifterna inte förvanskas eller förstörs eller att obehöriga kommer åt uppgifterna (integritet och konfidentialitet).

5.PRINCIPER FÖR BEHANDLING AV PERSONUPPGIFTER forts.

Du måste för att få behandla personuppgifter i din verksamhet kunna stödja behandlingen på någon av följande rättsliga grunder för laglig behandling.

- **samtycke**
- **avtal** med den registrerade
- fullgöra en **rättslig förpliktelse**
- för att skydda intressen av grundläggande betydelse för den registrerade eller annan fysisk person
- för att utföra en uppgift av allmänt intresse eller myndighetsutövning
- **intresseavvägning** (personuppgiftsansvariges berättigade intresse väger tyngre än den registrerades behov av integritet)

6. BARN OCH GDPR

De vanliga avtalsrättsliga reglerna gäller även vid personuppgiftsbehandling som gäller barn. Dessa innebär att den som är under 18 år som huvudregel inte kan teckna bindande avtal. Av samma anledning kan den som är under 18 år som huvudregel inte heller samtycka till behandling av sina personuppgifter. Det är den som har föräldraansvaret som kan lämna samtycke.

Om barnet är under 13 år är behandling av personuppgifter med stöd av samtycke t.ex. i appar eller sociala medier tillåten endast om samtycke ges eller godkänns av den som har föräldraansvar för barnet. Ditt företag ska kontrollera att samtycke ges eller godkänns av den som har föräldraansvaret. Ett undantag från huvudregeln ovan är att barn som minst är 13 år kan samtycka när det är fråga om appar m.m. som erbjuds direkt till ett barn som bor i Sverige. Den som när hen var minderårig har lämnat sitt samtycke till behandling av personuppgifter t.ex. i appar m.m. kan begära att uppgifterna ska raderas och även som vuxen begära att personuppgifterna ska raderas. Denna rätt för den som var minderårig när hen lämnade sitt samtycke till behandling av personuppgifter, att få sina personuppgifter raderade är ovillkorad, till skillnad mot rätten till radering i artikel 17 GDPR som ställer upp vissa villkor för rätt till radering av uppgifterna.

Om ditt företag använder intresseavvägning som rättslig grund för laglig behandling ska ni ta särskild hänsyn till barnets behov av integritet vid avvägningen. Information enligt GDPR som riktar sig till barn måste vara på ett tydligt och enkelt språk som barnet kan förstå.

7. KÄNSLIGA PERSONUPPGIFTER (SÄRSKILDA KATEGORIER AV PERSONUPPGIFTER)

Vissa personuppgifter är så känsliga att de som huvudregel bara får hanteras med den registrerades samtycke som rättslig grund. Ett giltigt samtycke ska dokumenteras och det är viktigt att det är lämnat uttryckligen, frivilligt och efter tillräcklig information så att den registrerade vet hur uppgifterna ska behandlas.

Känsliga personuppgifter är

- ras eller etniskt ursprung
- politiska åsikter
- religiös eller filosofisk övertygelse
- medlemskap i fackförening
- sexualliv eller sexuella läggning
- uppgifter om hälsa
- genetiska och biometriska uppgifter

I vissa undantagsfall krävs dock inte samtycke som t.ex. när den registrerade offentliggjort uppgifterna eller arbetsgivare behöver uppgifterna för att fullfölja sina arbetsrättsliga skyldigheter. Du måste därför inför att ditt företag behandlar känsliga personuppgifter alltid undersöka om du kan tillämpa något undantag eller om du kan få ett giltigt samtycke. Om ditt företag varken kan få ett giltigt samtycke eller kan tillämpa något undantag får företaget inte behandla de känsliga personuppgifterna.

8. REGISTER ÖVER PERSONUPPGIFTSBEHANDLINGAR

Ditt företag ska som personuppgiftsansvarig föra ett register över de behandlingar av personuppgifter som företaget ansvarar för.

Ett behandlingsregister ska innehålla följande

- kontaktuppgifter
- ändamål med behandlingen
- kategorier av registrerade och personuppgifter
- mottagare eller kategorier av mottagare av uppgifterna
- skyddsåtgärder om behandlas utanför EU/EES
- tidsfrist för radering
- beskrivning av säkerhetsåtgärder

När behandlingen av personuppgifter är tillfällig och det inte är fråga om känsliga personuppgifter behöver företag med färre än 250 anställda inte ta upp de tillfälliga behandlingarna i registret, om det inte finns någon risk för att den registrerades rättigheter och friheter äventyras.

Du hittar en enkel mall för behandlingsregister på Företagarnas webbplats.

9. INFORMATION TILL DE REGISTRERADE

De personer vars uppgifter ditt företag hanterar har rätt till information om behandlingen. Informationen ska lämnas inom en månad dock senast vid kommunikation eller utlämnande till någon annan.

Informationen ska lämnas

- när uppgifter samlas in
- när uppgifter hämtas från annan
- när uppgifterna ska användas för annat syfte än de samlades in för

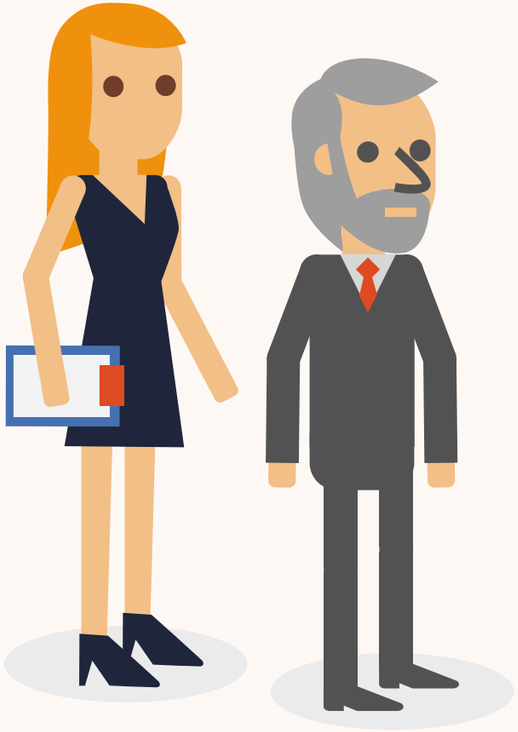
De uppgifter som ska lämnas är

- kontaktuppgifter till personuppgiftsansvarig (ditt företag) och ev. dataskyddsombud
- ändamålen med att behandla personuppgifterna
- den rättsliga grunden för användningen av personuppgifterna
- om rättsliga grunden är intresseavvägning beskriv det berättigade intresset för behandlingen
- kategorier av personuppgifter som hanteras
- mottagare av uppgifterna och mottagare i länder utanför EU/EES
- Information om skyddsåtgärder om uppgifterna kommer hanteras utanför EU/EES
- tid för lagring
- rätten till tillgång till uppgifterna, rättelse eller radering, begränsning av behandlingen rätten till dataportabilitet (att uppgifterna förs över till annan)
- rätten att återkalla samtycke
- att klagomål kan lämnas till Datainspektionen
- om uppgifterna måste lämnas enligt t.ex. lag eller avtal och följderna av om de inte lämnas

9. INFORMATION TILL DE REGISTRERADE forts.

- var uppgifterna kommer från
- om det sker automatiserat beslutsfattande eller profilering

Informationen ska vara koncis, klar och tydlig, begriplig och i en lätt tillgänglig form med användning av klart och tydligt språk. Detta innebär att du måste formulera informationen på ett sätt som mottagaren kan förstå och ta till sig. Ditt företag ska anpassa språket efter vem som ska få informationen. Det är tillåtet att använda symboler om det underlättar.



10. HANTERA REGISTRERADES RÄTTIGHETER

De personer vars personuppgifter ditt företag hanterar har vissa andra rättigheter som de kan utöva, utöver rätten till information. De har rätt att få reda på bl.a. vilka kategorier av uppgifter ditt företag behandlar om dem, rätt att få uppgifter rättade, i vissa fall rätt att få uppgifter raderade (rätten att bli glömd), invända mot att deras uppgifter behandlas i vissa fall, i vissa fall begränsa ditt företags behandling av deras uppgifter och i vissa fall få uppgifter överförda till annat företag (dataportabilitet).

När en registrerad begär tillgång till sina uppgifter ska ditt företag

- Kontrollera att det är den registrerade som begär ut uppgifterna
- Den registrerade har rätt att få reda på

– ändamålen,

– kategorier av personuppgifter som behandlas,

– mottagare eller kategorier av mottagare av personuppgifterna,

– hur länge uppgifterna behålls,

– rätten att begära rättelse, radering eller begränsning av eller invända mot behandlingen,

– rätten att klaga till Datainspektionen,

– information om den som uppgifterna hämtats från om de inte kommit från den registrerade,

– uppgift om ev. automatiserat beslutsfattande och profilering med information om logiken och förutsedda följder för den registrerade

– skyddsåtgärderna om uppgifterna hanteras utanför EU/EES.

- Svara skriftligen utan dröjsmål med informationen och kopia på personuppgifterna, senast inom en månad

10. HANTERA REGISTRERADES RÄTTIGHETER forts.

Om den registrerade begär att få en kopia på sina uppgifter mer än en gång får ditt företag ta ut en rimlig administrativ avgift.

När den registrerade begär rättelse ska ditt företag

- Rätta felaktiga uppgifter utan onödigt dröjsmål
- Komplettera ofullständiga uppgifter utan onödigt dröjsmål
- Meddela den registrerade om vidtagna åtgärder inom en månad

När den registrerade begär radering ska ditt företag

- Kontrollera att det är den registrerade som begär radering
- Undersöka om villkoren för rätt till radering är uppfyllda. Rätt till radering finns för den registrerade om:

– Behandlingen inte längre nödvändiga för ändamålet

– Den registrerade återkallat samtycke

– Den registrerade invänt mot marknadsföring och det saknas berättigade skäl som väger tyngre

– Om personuppgifterna behandlats olagligt

– Om radering krävs för att uppfylla rättslig förpliktelse

- Om samtycke lämnats av omyndig vid erbjudande av informationssamhällets tjänster (t.ex. samtycke i en app)
- Radera uppgifterna som ditt företag är skyldigt att radera
- Meddela den registrerade om vidtagna eller inte vidtagna åtgärder inom en månad. Motivera gärna tydligt om ni avstår från att radera uppgifterna.

10. HANTERA REGISTRERADES RÄTTIGHETER forts.

När den registrerade begär begränsning av behandlingen

- Kontrollera att det är den registrerade som begär begränsning av behandlingen
- Undersök om ditt företag bara får lagra, behandla uppgifterna med samtycke, ta tillvara sin rätt eller skydda annans rättigheter eller friheter p.g.a.

– period då korrektheten eller invändning mot intresseavvägning undersöks

– behandlingen är olaglig men registrerade motsätter sig radering

– ditt företag behöver inte uppgifterna men registrerade behöver dem för att ta tillvara sin rätt

- Meddela den registrerade om vidtagna eller inte vidtagna åtgärder inom en månad. Motivera gärna tydligt om ni inte begränsar behandlingen.

När den registrerade begär att personuppgifterna ska överföras till annan (dataportabilitet)

- Kontrollera att det är den registrerade som begär överföringen
- Undersök om ditt företag måste föra över uppgifterna om följande villkor är uppfyllda

– grund för behandling är samtycke eller avtal

– uppgifterna hanteras med automatiserad behandling och det är tekniskt möjligt att överföra uppgifterna och

– överföringen inte påverkar andras rättigheter och friheter ogynnsamt

- Meddela den registrerade om vidtagna eller inte vidtagna åtgärder inom en månad. Motivera gärna tydligt om ditt företag inte för över uppgifterna.

11. PERSONUPPGIFTSINCIDENT

Om personuppgifter oavsiktligt eller olagligt blir förstörda, ändrade eller obehöriga kommer åt uppgifterna kallas det för personuppgiftsincident. Om det inte är osannolikt att personuppgiftsincidenten medför risk för fysiska personers rättigheter och friheter ska incidenten anmälas till Datainspektionen inom 72 timmar från att ditt företag upptäckt incidenten. Detta gör du på en blankett som du hittar på Datainspektionens webbplats.

Även om du inte behöver anmäla incidenten ska ditt företag dokumentera incidenten.

Ditt företag ska informera de registrerade om incidenten sannolikt leder till hög risk för fysiska personers rättigheter och friheter (finns det risk att personens möjligheter, person eller egendom skadas?). Informationen till de registrerade ska innehålla minst

- namnet på och kontaktuppgifter till ev. dataskyddsombud eller annan kontakt på företaget
- de sannolika konsekvenserna av personuppgiftsincidenten
- ditt företags åtgärder med anledning av personuppgiftsincidenten och för att mildra möjliga negativa effekter

12. DATASKYDDSOMBUD

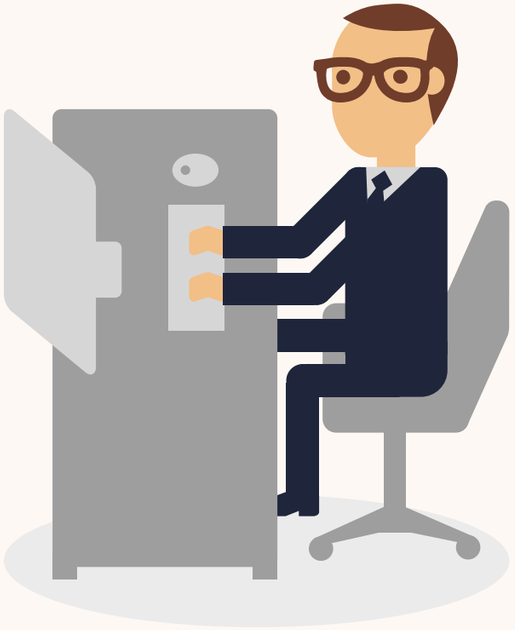
Ditt företag ska ha ett dataskyddsombud om kärnverksamheten är regelbunden och systematisk övervakning av de registrerade i stor omfattning eller hantering i stor omfattning av känsliga personuppgifter eller brott. Myndigheter ska alltid ha dataskyddsombud. Dataskyddsombudet är en person med särskilda kvalifikationer och sakkunskap men det är den personuppgiftsansvarige som har ansvaret för hanteringen av personuppgifter enligt GDPR.

Dokumentera skriftligen varför ditt företag inte utsett ett dataskyddsombud.

13. KONSEKVENSBEDÖMNING

Om en behandling av personuppgifter leder till hög risk för fysiska personers rättigheter och friheter ska ditt företag innan behandlingen påbörjas göra en bedömning av konsekvenserna. Exempel på när det behövs en konsekvensbedömning är omfattande behandling av känsliga personuppgifter och systematisk övervakning av allmän plats. Om ditt företag inte kan garantera säkerheten kan ni samråda med Datainspektionen. Du kan läsa mer om konsekvensbedömning och förhandsamråd m.m. på Datainspektionens webbplats.

Där hittar du också Datainspektionens lista med vilka som måste göra en konsekvensbedömning.



14. GDPR OCH MARKNADSFÖRING

Företag måste följa GDPR även när de behandlar personuppgifter i samband med marknadsföring. I Sverige är det marknadsföringslagen som reglerar hur och när marknadsföring får ske. GDPR i sin tur reglerar hur personuppgifterna får behandlas i samband med själva marknadsföringen. En behandling av personuppgifter vid marknadsföring kan t.ex. vara att en samling med e-postadresser används för marknadsföring per e-post.

Marknadsföringsreglerna i enlighet med marknadsföringslagen i korthet

Marknadsföringslagen skiljer på marknadsföring som riktas mot konsumenter (fysiska personer) och företag (juridiska personer). Lagen ställer högre krav på marknadsföring riktad mot privatpersoner än mot företag. Vid sidan om de generella reglerna om att marknadsföring inte får vara aggressiv och vilseledande finns det specifika regler kring när olika medier får användas.

E-post och sms-marknadsföring riktad mot konsument

Huvudregeln är att du enbart får använda dig av e-post och sms-marknadsföring gentemot konsument då denne givit dig lov. Undantaget är om konsumenten sedan tidigare handlat av dig och det rör sig om liknande varor/tjänster och inte i övrigt motsatt sig marknadsföring. Det ska på ett enkelt sätt finnas möjlighet att avbeställa marknadsföringen, t.ex. genom en länk i e-postmeddelandet.

E-post och sms-marknadsföring till företag

Till företag får du fritt använda dig av e-post och sms enligt marknadsföringslagen. Tänk dock på att reglerna i GDPR fokuserar på om det är behandling av personuppgift eller inte och skiljer inte på så sätt mellan företag och privatperson. GDPRs regler kan gälla för t.ex. en e-postadress eller ett personnamn som behandlas av den personuppgiftsansvarige, även om dessa kopplade till ett företag.

14. GDPR OCH MARKNADSFÖRING forts.

Rättslig grund för att behandla personuppgifter vid marknadsföring

I de allra flesta fall är det den lagliga grunden intresseavvägning som tillämpas vid behandling av personuppgifter vid marknadsföring, d.v.s. intresset som ditt företag har för att få marknadsföra ditt företags varor och tjänster är större än mottagarens intresse av integritet. Finns det exempelvis en pågående affärsrelation mellan er kan avtal vara en annan rättslig grund att använda sig av. Att tillämpa samtycke i marknadsföringssammanhang skulle givetvis också gå, tänk dock på att samtycken går att återkalla.

Måste mottagarna av marknadsföring få en personuppgiftspolicy?

Om du är personuppgiftsansvarig, d.v.s. den som bestämmer ändamål och medel för hur personuppgifterna används, ska du ge mottagarna information kring hur deras personuppgifter behandlas som redogjorts för i tidigare avsnitt. Om marknadsföringen sker genom ett e-postmeddelande kan informationen ske genom att du t.ex. också skickar över din personuppgiftspolicy i samband med marknadsföringen

15. VAD BEHÖVER ETT FÖRETAG GÖRA?

Det kan kännas överväldigande att för en företagare att följa alla regler kring hantering av personuppgifter. Men genom att läsa denna skrift har du redan kommit igång med att skaffa dig kunskap. Nedan har du en punktlista över vad ditt företag bör göra för att kunna följa reglerna:

- skaffa kunskap och se till att alla som hanterar personuppgifter har rätt kunskap
- inventera och kartlägg hur ditt företag hanterar personuppgifter och se till att detta följer reglerna
- gör ett register över behandlingarna av personuppgifter som sedan uppdateras kontinuerligt
- se till att det finns sparade skriftliga samtycken när det används som rättslig grund för behandling av personuppgifter
- ta fram och uppdatera information till de registrerade och se till att det finns en rutin kring detta så att informationen lämnas till den registrerade enligt GDPR
- ändrade/nya rutiner för att kunna i rätt tid svara registrerade när de tar tillvara sina rättigheter enligt GDPR
- om ditt företag ingår avtal som innebär hantering av personuppgifter så ta upp det i avtalet t.ex. om det behövs ett personuppgiftsbiträdesavtal eller de registrerade ska informeras om ett utlämnade
- ha rutin för hantering av personuppgiftsincidenter
- utse dataskyddsombud alternativt dokumentera varför företaget avstår från att utse dataskyddsombud
- om det behövs göra konsekvensbedömningar

15. VAD BEHÖVER ETT FÖRETAG GÖRA?

- ta in överväganden om hantering av personuppgifter i det löpande arbetet och löpande uppdatera register över behandlingarna, information till registrerade, rutiner m.m.

Du kan hittar mall för behandlingsregister och personuppgiftsbiträdesavtal och även annan information om GDPR på Företagarnas webbplats. Du hittar även information om hantering av personuppgifter på Datainspektionens webbplats.

Ett företags personuppgiftshantering är ett arbete som ständigt måste uppdateras och förbättras med hänsyn till utvecklingen i företaget, samhället och av tekniken som används. Genom att följa reglerna i GDPR skyddar ditt företag den personliga integriteten för alla som kommer i kontakt med ditt företag. När ditt företag gör det på rätt sätt har företaget nytta av detta arbete.

Det här är Företagarna

Vi är Sveriges största intresseorganisation för dig som är företagare. Vi företräder 60 000 företagare i Sverige. Det ger oss kraft att påverka makthavare på alla plan och i många frågor. Som medlem i Företagarna får du även en rad förmåner och erbjudanden som gör din företagarvardag enklare och roligare.

social med oss!

67 Stockholm Växel: 08 406 17 00 | foretagarna.se