GDPR-guide

FÖR LÖNEADMINISTRATÖREN

VISMA

GDPR på lönekontoret

Det här är en översiktlig introduktion för vad du behöver tänka på när det gäller anställningar och GDPR, eller Dataskyddsförordningen som det svenska namnet är. Detta är inte en juridisk handbok utan snarare en smidig checklista med några tips.

HUR PÅVERKAS LÖNEKONTORET/ HR-AVDELNINGEN?

Som arbetsgivare har du ansvar för att ge information när du samlar in personuppgifter, till exempel vid rekrytering eller anställning. Du måste skydda de personuppgifter du behandlar, hålla dem uppdaterade och se till att ta bort dem när de inte behövs längre.

LITE OM LAGEN

Vi börjar med en kort genomgång av några begrepp.

PERSONUPPGIFTER, VAD ÄR DET?

En personuppgift är allt som direkt eller indirekt säger något om en nu levande fysisk person. Direkta uppgifter är naturligtvis kontaktuppgifter som namn och adress, telefonnummer och e-postadress. Det är också fotografier som ju kan säga mycket om den avbildade.

Bland de indirekta uppgifterna hittar vi ip-adress (datorns identitet), registreringsnummer på bilen och mycket annat man kanske inte tänker på. Skillnaden mellan en privatbil och en firmabil framgår om man frågar bilregistret som registrerar ägarna. Därför är registreringsnummer en personuppgift.

NÄR FÅR JAG BEHANDLA PERSONUPPGIFTER?

Om du samlar in personuppgifter måste du först informera om vilka uppgifter du vill ha, vad du ska ha dem till (syfte) och när du tänker radera dem. Du ska också informera om vem du är och om de rättigheter den registrerade har.

Du måste också berätta med vilken rätt du tänker behandla uppgifterna, den rättsliga grunden. Det finns sex stycken grunder att välja på i lagen. Uppfyller du inte någon av dem så är det förbjudet att behandla andras personuppgifter.

De rättsliga grunderna är:

- Samtycke
- Avtal
- Rättslig förpliktelse
- Grundläggande (vital) betydelse
- Allmänt intresse eller myndighetsutövning
- Intresseavvägning

http://www.privacy-regulation.eu/sv/6.htm

"GALLRA" – ETT NYCKELORD

När du inte längre har rätt att behandla vissa personuppgifter så ska de tas bort. Det kan ske genom att du raderar dem eller att du anonymiserar dem. Kravet är att de inte ska gå att återställa eller att du genom uppgifter somt ex ort + yrke kan räkna ut vem det är.

Rekrytering

Låt oss prata lite om hantering av personuppgifter i samband med rekrytering. Här är några saker du bör tänka på.

- Personuppgifter i en ansökan, intervju-anteckningar och uppgifter från referenser får registreras och sparas så länge de är nödvändiga för ansökningsförfarandet. Därefter ska uppgifterna gallras.

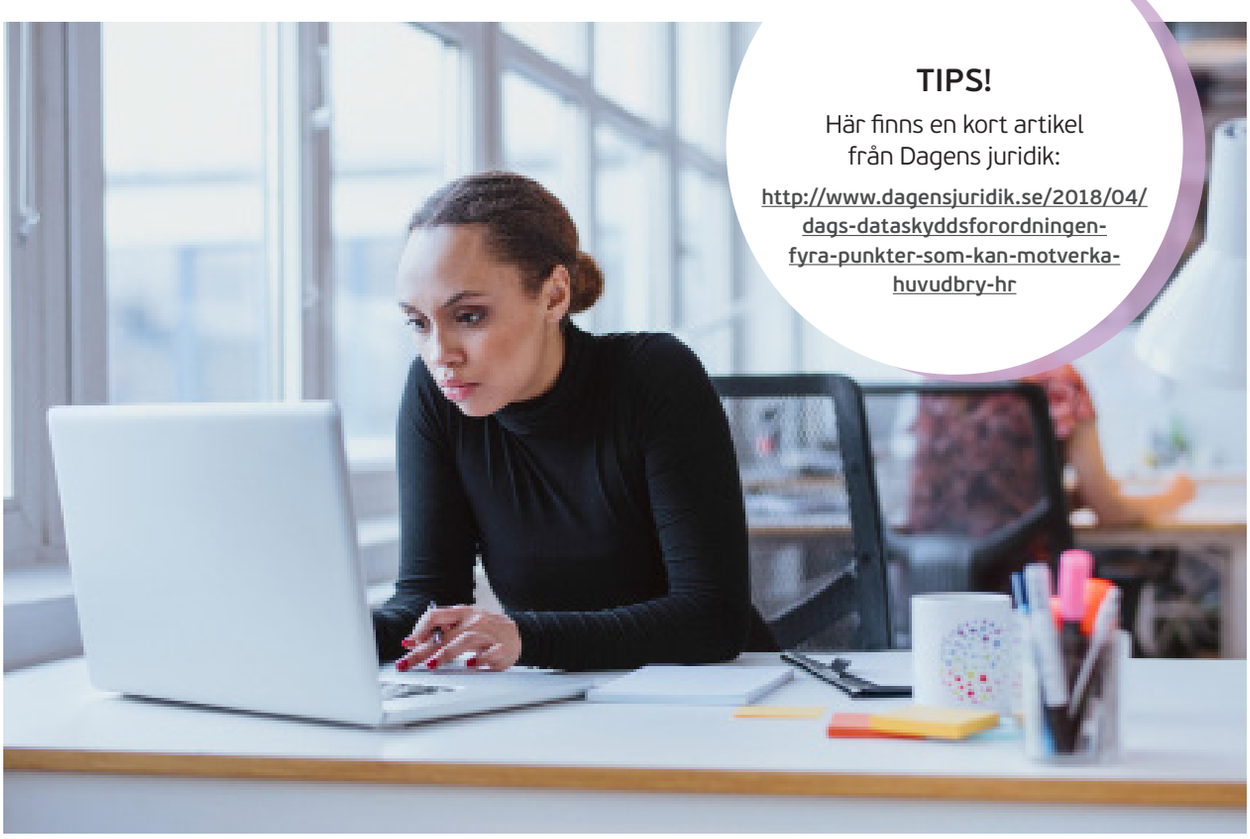
- Det är klokt att inte begära in fler uppgifter än du verkligen behöver.

- Tänk också på hur du sprider uppgifterna internt, exempelvis en kopia till rekryterande chef eller en kopia till någon annan. Du måste ha kontroll på var kopiorna finns och att de förstörs när de inte längre behövs, såväl papperskopior som bilagor i e-posten.

- Arbetsgivaren får dock spara uppgifterna så länge sökande som inte har anställts kan vidta rättsliga åtgärder, till exempel om man inte fått jobbet och vill överklaga. Här vill vi påminna om Diskrimineringslagen som säger att man kan överklaga upp till 2 år efter tjänsten tillsattes.

- Om uppgifterna ska sparas under en längre tid för framtida rekrytering krävs den sökandes samtycke. Tänk dock på att du i så fall bygger upp ett personregister och är skyldig att hålla det uppdaterat med korrekta uppgifter. Du kan till exempel mejla de registrerade en gång om året och fråga om de vill stå kvar samt om deras uppgifter stämmer. Tänk på att inte mejla personnummer.

- Formulera en rutin för rekryteringsprocessen och skriv ner den. Då blir det lättare att göra rätt i framtiden.



TIPS!

Här finns en kort artikel från Dagens juridik:

http://www.dagensjuridik.se/2018/04/dags-dataskyddsforordningen-fyra-punkter-som-kan-motverka-huvudbry-hr

Anställning

Vid anställning är det en del saker du behöver ha koll på. Här går vi igenom steg för steg.

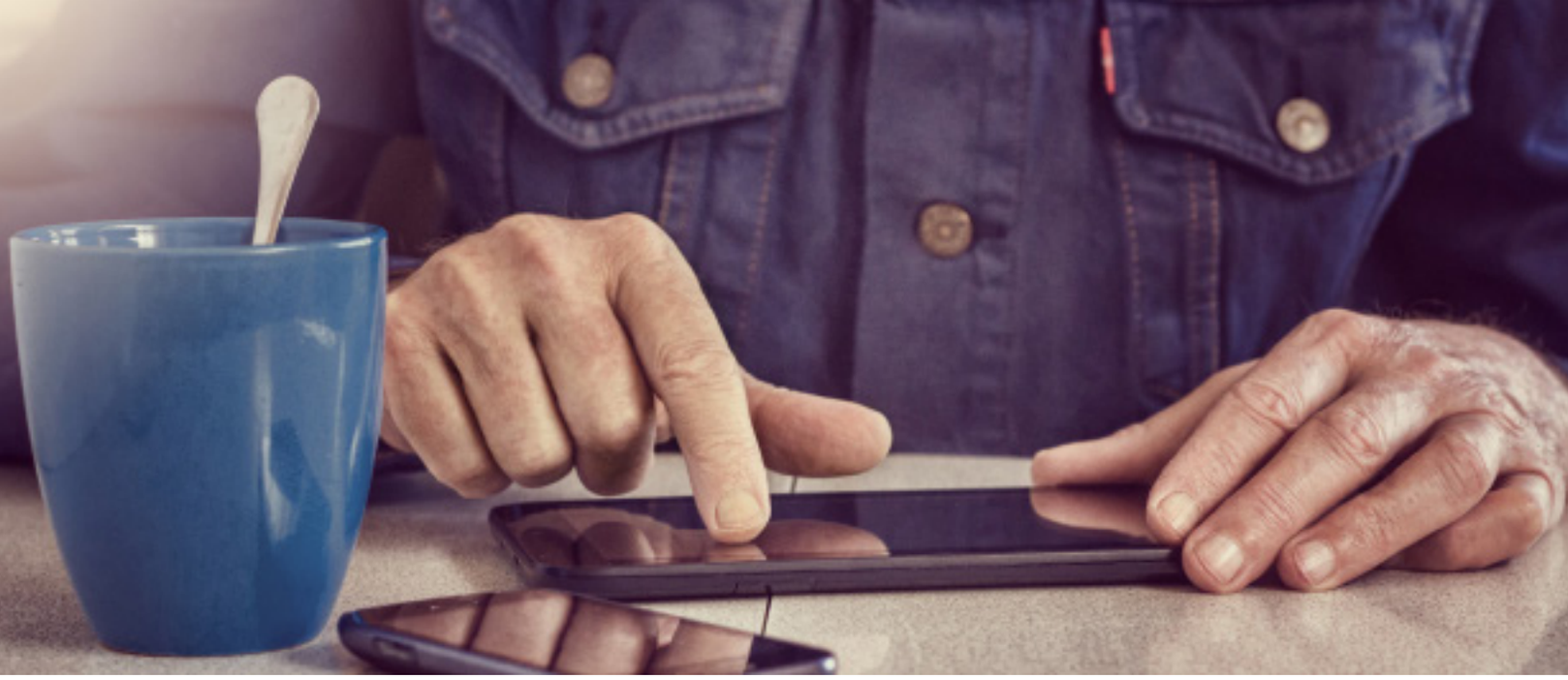
Steg 1: När anställnings-avtalet ingås

INFORMATION

Informationskraven i GDPR gäller alla, också anställda. Du måste alltså informera om vilka personuppgifter, eller kategorier av personuppgifter, du samlar in, vad du tänker göra med dem (syfte), med vilket rättsligt stöd du behandlar olika uppgifter och när du avser att sluta behandla dem (ta bort dem). Detta ska göras innan du samlar in uppgifterna, alltså i praktiken när du ingår anställningsavtalet. Det kan vara lämpligt att skicka informationen när du meddelar att den sökande fått tjänsten. Om ni har ett intranät så bör informationen också finnas där tillsammans med andra policies/personalinformation.

Ett exempel från Datainspektionen kan ge en antydan om kravet på noggrannhet:

Ändamålet var inte tillräckligt angivet
”Datainspektionen ansåg i ett ärende att det inte var tillräckligt att enbart ange att ”kontroll och loggning kan förekomma” som ändamål för loggning och övervakning på ett sjukhus utan att man samtidigt angav vad syftet med denna kontroll var. Till exempel kan ett sådant syfte vara att man vill övervaka de anställdas arbete för att senare göra en uppföljning av att de interna reglerna följs.” Glöm inte heller att informera om ni använder ”molnbaserade” program, exempelvis för e-post och om data kommer att överföras till någon utanför EU/EES (Tredje land). Ni är skyldiga att ha personuppgiftsbiträdesavtal med era underleverantörer och informationen kan innehålla uppgiften att ni alltid upprätthåller skyddet genom sådana avtal och av EU godkända avtal med företag i ”tredje land”.



Steg 2: Första tiden

Eftersom företaget är ansvarigt för personuppgifter ni får er anförtrodda behöver ni se till att en nyanställd får kunskap om Dataskyddslagen och hur ni hanterar den i er verksamhet. Det kommer att skilja mycket mellan olika företag beroende på hur ni behandlar personuppgifter så fundera på vilket sätt som passar er.

Det är lätt att inse att de som ofta har direkt kundkontakt behöver utbildning men glöm inte att personuppgifter också kan vara åtkomliga för de som administrerar era datasystem.

Steg 3: Samtycke

Samtycke ska vara frivilligt, välinformerat och tydligt. Lagen säger också att "Samtycke bör inte betraktas som frivilligt om den registrerade inte har någon genuin eller fri valmöjlighet eller inte utan problem kan vägra eller ta tillbaka sitt samtycke."

Det betyder att maktförhållandet mellan arbetsgivaren och den anställde gör att samtycke i många fall inte kan anses giltigt. Det kan användas i fall där det inte finns något annat alternativ. Ett exempel kan vara om man vill publicera bild på en anställd på internet.

Steg 4: Anhöriga

Får en arbetsgivare registrera kontaktuppgifter till anhöriga?

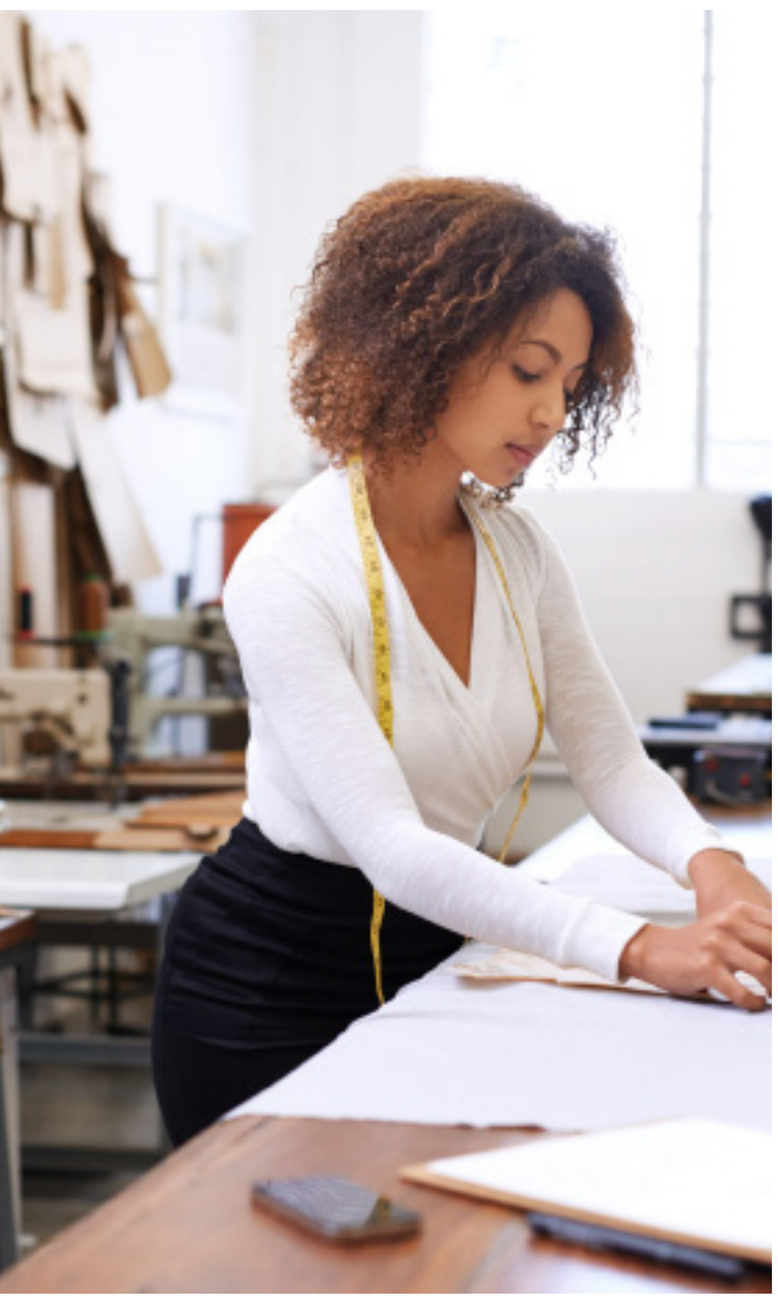
Så här svarar Datainspektionen:
Ja, arbetsgivaren har ofta ett starkt intresse av att kunna kontakta anhöriga vid till exempel olycksfall eller sjukdom. Arbetsgivarens intresse av att från sina anställda samla in och registrera anhörigas namn och kontaktuppgifter väger över de registrerades intresse av att uppgifterna inte behandlas. Därför behöver inte samtycke hämtas från de anhöriga eftersom behandlingen kan ske efter en intresseavvägning.

Personuppgifter som behandlas måste vara riktiga och aktuella, därför behöver arbetsgivaren ha rutiner för att uppdatera uppgifterna. Det kan ske genom att helt enkelt fråga de anställda om uppgifterna är aktuella eller att låta den anställde själv ändra sin kontaktinformation när förhållandena ändras.

Arbetsgivaren behöver också ha en rutin för att informera de anhöriga, till exempel genom att den anställde får en informationslapp att ta hem. Arbetsgivaren behöver även begränsa åtkomsten till uppgifterna så att den bara omfattar befattningshavare som har till uppgift att kontakta anhöriga.

Steg 5: Lönearbetet

För företagets arbete med löner och personalfrågor finns det ett antal frågor att reda ut. Här redogör vi för de allra viktigaste delarna du behöver hålla koll på som löneadministratör.



HUR SKICKAR JAG LÖNEBESKEDEN UTAN ATT ANVÄNDA E-POST?

E-post är inte en säker kommunikationsform då lönebesked ofta innehåller uppgift om sjukfrånvaro. Detta är en uppgift om personens hälsa och därmed en känslig personuppgift. Känsliga uppgifter får inte behandlas utan starkt skydd.

I vårt löneprogram **Visma Lön** rekommenderar vi tjänsten Mitt Lönebesked som skickar digitala lönebesked på ett säkert sätt. Anställda kan sedan välja att ta emot sitt lönebesked på webben i Mitt Lönebesked eller i mobilappen Min Lön.

HUR SPARAR JAG UTSKRIFTER FRAMÖVER?

En nyhet i GDPR är att lagen också gäller ostrukturerat material, exempelvis e-post och dokument. Du måste alltså tänka igenom om du bara sparar sådant som är nödvändigt och om du förvarar det säkert. Du behöver också en rutin för att regelbundet gå igenom och ta bort material du inte längre behöver. Tänk på att papper i en pappersinsamling är helt oskyddade och dessutom sprids utanför företaget. Kanske är det dags att sluta lagra papper utan spara dokumenten i datorn istället?

BEHÖVER VI ÄNDRA I VÅR MALL FÖR ANSTÄLLNINGSAVTAL?

Anställningsavtal kan se ut på många olika sätt. Om ni använder en avtalsmall ”av gammal vana” så är det en bra idé att se över den nu.

Det finns ett starkt arbetsrättsligt krav på sekretess och lojalitet men det kan vara en bra idé att inkludera en sekretessklausul om ni inte redan har sekretessavtal på plats. Då blir det tydligt att företaget lägger stor vikt vid hantering av personuppgifter.

Några saker till om personalarbetet

KÄNSLIGA UPPGIFTER

Många av oss har en klar uppfattning om vad vi anser är känsliga uppgifter. Bankkontonummer och lön är ett par exempel. Men i lagens mening är det bara sju olika kategorier som är "känsliga" och medför ännu striktare krav på hur de behandlas.

Det är uppgifter om:

- Ras eller etniskt ursprung
- Politiska åsikter
- Religiös eller filosofisk övertygelse
- Medlemskap i fackförening
- Genetiska och biometriska uppgifter
- Hälsa
- Sexuell läggning

SJUKDOM, ALLERGI MM

När du arrangerar ett evenemang där mat ingår är det viktigt att du får veta om det är något de anmälda inte tål. Sådan information behöver också vidarebefordras till restauranten eller cateringföretaget. Det är uppgifter du får med den registrerades samtycke.

När evenemanget sedan är över ska uppgifterna tas bort. Om den registrerade, exempelvis en anställd, uttryckligen begär att du ska spara uppgiften så kan du göra det. Tänk dock på att du ska kunna bevisa samtycket så med största sannolikhet behöver det vara skriftligt.

Restaurangen behöver vanligtvis bara veta antal portioner av olika slag när du beställer, men om de måste få veta i förväg vem som ska ha vad ska ni försäkra er om att de raderar uppgifterna efteråt.

RÄTT ATT BLI GLÖMD

En nyhet i GDPR är att den registrerade har "Rätt till radering".

Rätten att bli glömd gäller (huvudsakligen):

- Om uppgifterna inte längre är nödvändiga för de syften du uttalat.
- Uppgifter som behandlas med samtycke om samtycket återkallas.
- Uppgifter som behandlas efter intresseavvägning om den registrerade ifrågasätter avvägningen och får rätt.
- Om uppgifterna behandlas på olagligt sätt.

Om det skulle finnas en annan rättslig grund för behandling av vissa uppgifter så behöver du inte radera de uppgifterna. Ett bra exempel är alla uppgifter som skapas vid lönekörningar. De har företaget skapat och de är företagets "egendom". Olika arbetsrättsliga lagar, bokföringslagen samt företagets egna behov ger rättsliga grunder och tidsgränser för behandlingen.

Anställningens upphörande

VILKA UPPGIFTER BEHÖVER JAG SPARA/ TA BORT NÄR EN ANSTÄLLD SLUTAR?

En hel del uppgifter ingår i redovisningen och ska sparas 7 år enligt Bokföringslagen. Det kan också finnas andra lagar eller avtal som påverkar. Uppgifter om anhöriga bör raderas omedelbart.

Det är god sed att arbetsgivaren kan lämna ett anställningsbevis och vi vet nog alla att ett sådant önskemål kan komma sent. Företaget vill kanske också bevara sin historia under en viss tid. Läs mer om hur länge man bör och får spara olika uppgifter i vår artikel "Gallringstider för löneavdelningen", https://vismaspcs.se/ditt-foretagande/sakerhet/gallring-gdpr-lon.

Exempel: Om någon hör av sig kan de meddela vart man ska skicka intyget. Det finns alltså ingen anledning att spara en persons adress av det skälet. Datainspektionen säger så här:

"Betyg och tjänstgöringsintyg med omdömen som arbetsgivaren har gett till arbetstagaren får sparas. Det är däremot inte tillåtet att vid sidan av sådana intyg spara värderande uppgifter utan den anställdes samtycke. Samtycket måste föregås av tydlig information där arbetsgivaren anger vilka kategorier av uppgifter som ska sparas.

Arbetsgivaren får spara rena faktauppgifter som "uppsägning på grund av arbetsbrist", "avsked" och "uppsägning på grund av personliga skäl". Uppgifter får sparas för administrativa ändamål och även för att kunna lämna referenser till andra arbetsgivare.

Arbetsgivaren får behålla uppgifter under den tid som en tvist med en tidigare anställd kan bli aktuell. Om en anställd har sagts upp på grund av arbetsbrist måste arbetsgivaren spara uppgifter för att bevaka företrädesrätt till ny anställning. Man får spara uppgifter som behövs för att avgöra om personen har tillräckliga kvalifikationer för en ny befattning."

Sveriges småföretag använder program från Visma Spcs.

Mer än hälften av landets småföretag som använder ett bokförings- eller ett fakturerings-program har valt Visma. Av våra nya kunder väljer mer än 75 % en webbaserad lösning. Att vi är marknadsledande är en trygghet för dig.

VISMA SPCS AB
Sambandsvägen 5, 351 94 Växjö
0470-70 60 00 • infoline@vismaspcs.se
vismaspcs.se