Europeiska kommissionen

Sju steg att ta för företag

som vill förbereda sig inför den allmänna dataskyddsförordningen (GDPR)

Rättsliga frågor och konsumentfrågor

Vem riktar sig detta till?

Syftet med den här guiden är att hjälpa de företag som inte hanterar personuppgifter som en grundläggande affärsverksamhet, t.ex. små och medelstora företag som främst bara har hand om personuppgifter för sina anställda eller har listor över kunder och klienter. Det innefattar bland annat affärsidkare eller butiker, till exempel bagerier eller slakterier, eller tjänsteleverantörer såsom arkitekter. Den här guiden betonar de få åtgärder som behöver tas för att förbereda sig inför GDPR.

Personuppgifter är all information som gäller en faktisk levande enskild person (ej juridiska personer). Det innefattar t.ex. namn, efternamn, hemadress, e-postadress eller platsuppgifter från kartan på din mobil. Normalt är det på det sättet med de uppgifter du kanske har om dina anställda, dina kunder eller leverantörer.

Ju mindre risk din verksamhet utgör för personuppgifter, desto mindre behöver du göra

Tillämpa huvudprinciperna:

- **Samla in personuppgifter med ett tydligt definierat syfte, och använd dem inte till något annat** (om du ber dina kunder att ge dig sin e-postadress så att de kan få dina nya erbjudanden eller kampanjutskick, så kan du inte använda den e-postadressen till något annat eller sälja den till ett annat företag).
- **Samla inte fler uppgifter än du behöver** (om du gör hemleveranser behöver du t.ex. en adress och ett namn på den som ringde, men du behöver inte veta om den personen är gift eller ogift). Var helt enkelt eftertänksam med de personuppgifter som du förfogar över.

STEG 1 KONTROLLERA DE PERSONUPPGIFTER DU SAMLAR IN OCH BEHANDLAR, I VILKET SYFTE DU GÖR DET OCH MED VILKEN RÄTTSLIG GRUND

Du har **anställda**; du behandlar deras personuppgifter utifrån anställningsavtalet och utifrån juridiska skyldigheter (t.ex. att rapportera till skattemyndigheterna/det sociala systemet).

Du kan förvalta en lista över **enskilda kunder**, t.ex. för att skicka dem meddelanden om specialerbjudanden/reklam om du fått samtycke från dessa kunder.

Du behöver inte alltid samtycke. Det finns fall då enskilda personer förväntar sig att du behandlar deras uppgifter. Som pizzabud kan du t.ex. behandla leveransadressen för att annonsera en av dina nya produkter. Det kallas för ett berättigat intresse. Du måste informera enskilda personer om din avsedda användning och sluta behandla sådana uppgifter om de säger åt dig att göra det.

Om du förvaltar en lista över **leverantörer** eller **företagskunder**, så gör du det utifrån de avtal du har med dem. Avtalen är inte nödvändigtvis i skriftlig form.

STEG 2 INFORMERA DINA KUNDER, ANSTÄLLDA OCH ANDRA ENSKILDA PERSONER NÄR DU SAMLAR IN DERAS PERSONUPPGIFTER

Enskilda personer måste känna till att du behandlar deras personuppgifter och i vilket syfte.

Det finns dock inget behov av att informera enskilda personer när de redan har information om hur du kommer att använda uppgifterna, t.ex. när en kund ber dig göra en hemleverans.

Du måste också på begäran informera enskilda personer om de personuppgifter du innehar om dem och ge dem tillgång till deras uppgifter. Ha dina uppgifter i ordning, så att du när t.ex. någon av dina anställda frågar dig vad du har för slags personuppgifter lätt kan ta fram dem utan extra krångel.

STEG 3 BEHÅLL PERSONUPPGIFTERNA BARA SÅ LÄNGE DET ÄR NÖDVÄNDIGT

Uppgifter om dina anställda: så länge anställningsförhållandet varar och enligt de medföljande juridiska skyldigheterna.

Uppgifter om dina kunder: så länge kundförbindelsen varar och enligt de medföljande juridiska skyldigheterna (t.ex. för skatteändamål).

Ta bort uppgifterna när de inte längre är nödvändiga för de ändamål du samlade in dem för.

STEG 4 SÄKRA DE PERSONUPPGIFTER DU BEHANDLAR

Om du behandlar dessa uppgifter i ett **IT-system**, ska du begränsa tillgången till filerna som innehåller uppgifterna, t.ex. med ett lösenord. Uppdatera regelbundet systemets säkerhetsinställningar.

(Notera: i GDPR föreskrivs inte att du ska använda något särskilt IT-system)

Om du lagrar fysiska dokument med personuppgifter, se då till att inga obehöriga kan komma åt dem; lås in dem i ett kassaskåp eller annat skåp.

STEG 5 BEHÅLL DOKUMENTATION OM DINA AKTIVITETER MED UPPGIFTSBEHANDLING

Sammanställ ett kort dokument där du förklarar vilka personuppgifter du behåller och av vilka anledningar. Du kan behöva göra dokumentationen tillgänglig för din nationella dataskyddsmyndighet när den begär det.

Sådana dokument bör innehålla den information som anges nedan.

INFORMATION	EXEMPEL
Ändamålet med databehandlingen	Meddela kunder om specialerbjudanden/tillhandahålla hemleverans; betala leverantören; löner och sociala avgifter för anställda
Typerna av personuppgifter	Kontaktuppgifter till kunder; kontaktuppgifter till leverantörer; uppgifter om anställda
Kategorierna av berörda registrerade	Anställda; kunder; leverantörer
Kategorierna av mottagare	Arbetsmarknadsmyndigheter; skattemyndigheter
Lagringsperioderna	Anställdas personuppgifter fram tills anställningsavtalet upphör (och tillhörande juridiska skyldigheter); kundernas personuppgifter tills kund-/avtalsförbindelsen upphör
De tekniska och organisatoriska säkerhetsåtgärderna för att skydda personuppgifterna	Om IT-systemlösningarna uppdateras regelbundet; låst skåp/kassaskåp
Om personuppgifter överförs till mottagare utanför EU	Användning av en processor utanför EU (t.ex. för lagring i molnet)

STEG 6 SÄKERSTÄLL ATT DIN UNDERLEVERANTÖR RESPEKTERAR REGLERNA

Om du lägger ut behandling av personuppgifter till ett annat företag, ska du bara använda en tjänsteleverantör som garanterar behandling i enlighet med kraven i GDPR (t.ex. säkerhetsåtgärder).

Innan du ingår ett avtal ska du kontrollera om de redan har gjort ändringar och anpassat sig efter GDPR. Ta med det i avtalet.

STEG 7 KONTROLLERA OM DU BERÖRS AV VILLKOREN NEDAN

> För att bättre skydda personuppgifter kan organisationer behöva utse ett dataskyddsombud. **Du behöver emellertid inte utse något dataskyddsombud** om behandling av personuppgifter inte är en grundläggande del av din verksamhet, om den inte är en riskfylld behandling och din verksamhet inte är i stor skala.

Om ditt företag exempelvis bara samlar uppgifter om dina kunder för hemleverans, så behöver du inte utse något dataskyddsombud.

Även om du faktiskt behöver använda dig av ett dataskyddsombud, så kan han/hon vara en befintlig anställd som får den funktionen utöver sina vanliga uppgifter. Eller så kan det vara en utomstående konsult, på samma sätt som många organisationer använder sig av externa revisorer.

> **Du behöver normalt inte utföra någon konsekvensbedömning avseende dataskydd**

En sådan konsekvensbedömning är förbehållen dem som utgör en större risk för personuppgifter, t.ex. när man utför storskalig övervakning av ett offentligt tillgängligt område (t.ex. videoövervakning).

Om ni är ett litet företag som hanterar anställdas löner och en lista över kunder, behöver du inte utföra någon konsekvensbedömning avseende dataskydd för dessa behandlingsåtgärder.

Böter

Tillsynsmyndigheterna för dataskydd har befogenhet att utfärda sanktioner vid brott mot dataskyddsreglerna. De kan anta korrigerande åtgärder (t.ex. ett åläggande eller en tillfällig indragning av behandlingen) och/eller utfärda böter.

Deras beslut att ge böter måste vara proportionellt och bygga på en bedömning av samtliga omständigheter i det enskilda fallet.

Om de bestämmer sig för att ge böter, kommer bötesbeloppet också att bero på omständigheterna vid fallet, däribland brottets allvarlighetsgrad eller om brottet var avsiktligt eller berodde på försummelse. De tar också hänsyn till din inställning och dina avsikter.

Om du vill ha mer information:

1. Besök Europeiska kommissionens vägledning till dataskyddsreformen online – finns på samtliga EU-språk:

https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_sv

2. Rådfråga din nationella dataskyddsmyndighet:

http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612080

VIKTIGT MEDDELANDE

Informationen i denna guide är avsedd att bidra till en bättre uppfattning om EU:s dataskyddsregler.

Detta är enbart menat som vägledning – endast texten i den allmänna dataskyddsförordningen (GDPR) har rättslig verkan. Till följd av detta är det enbart den allmänna dataskyddsförordningen som kan skapa rättigheter och skyldigheter för privatpersoner. Denna vägledning ger därför inte upphov till någon verkställbar rättighet eller förväntan.

Att göra bindande tolkningar av EU-lagstiftningen är Europeiska unionens domstols exklusiva befogenhet. De åsikter som uttrycks i denna vägledning ska inte ses som en förhandsdom av den ställning kommissionen kan tänkas ta inför EU:s domstol.

Varken Europeiska kommissionen eller någon person som agerar på Europeiska kommissionens vägnar är ansvarig för hur informationen i denna guide kan komma att användas.

Eftersom detta dokument speglar situationen när det författades, ska det ses som ett ”levande verktyg” som är öppet för förbättringar, och dess innehåll kan komma att ändras utan förvarning.

Publikationsbyrån

Luxemburg: Europeiska unionens publikationsbyrå, 2018

Print	PDF
ISBN 978-92-79-85381-4	ISBN 978-92-79-85378-4
doi:10.2838/42509	doi:10.2838/400931
DS-02-18-544-SV-C	DS-02-18-544-SV-N