Europeiska kommissionen

Den allmänna dataskyddsförordningen: nya möjligheter, nya skyldigheter

Vad varje företag behöver veta om EU:s allmänna dataskyddsförordning (GDPR)

Rättsliga frågor och konsumentfrågor

Printed by Bietlot in Belgium

Luxemburg: Europeiska unionens publikationsbyrå, 2018

Print	ISBN 978-92-79-79454-4	doi:10.2838/848923	DS-01-18-082-SV-C
PDF	ISBN 978-92-79-79414-8	doi:10.2838/66178	DS-01-18-082-SV-N

INNEHÅLLSFÖRTECKNING

KAPITEL 1

EN AFFÄRSMÖJLIGHET

Den allmänna dataskyddsförordningen (GDPR) reglerar hur företag behandlar och hanterar personuppgifter. Förordningen börjar gälla den 25 maj 2018 och gäller alla företag och organisationer (t.ex. sjukhus, offentlig förvaltning osv.). Den utgör den största förändringen av EU:s dataskyddsregler på 20 år.

Den allmänna dataskyddsförordningen ger medborgarna mer kontroll över hur deras personuppgifter används, men den strömlinjeformar dessutom regelverksförhållandena för företagen på ett markant sätt. Detta genom att det inrättas en enhetlig ram för dataskyddslagstiftning i hela EU. Man kan också säga att istället för att varje land har sina egna dataskyddslagar, så styrs nu hela EU av en enda förordning. På så sätt behöver ett företag som är verksamt i olika länder inte längre följa flera stycken – ofta olika – regelverk. Istället behöver de bara följa den allmänna dataskyddsförordningen för att kunna erbjuda sina tjänster var som helst i EU.

Hur den allmänna dataskyddsförordningen kan gynna ditt företag

- **En union, en lagstiftning:** en enda uppsättning regler gör det enklare och billigare för företag att göra affärer i EU.
- **En enda kontaktpunkt:** i de flesta fall behöver företagen bara ha att göra med en dataskyddsmyndighet.
- **EU-regler på EU:s mark:** företag som är baserade utanför EU måste tillämpa samma regler som företag i EU när de erbjuder sina varor eller tjänster till enskilda personer i EU.
- **Riskbaserat arbetssätt:** den allmänna dataskyddsförordningen undviker att alla hamnar under samma betungande plikt, och anpassar istället skyldigheterna efter de respektive riskerna.
- **Regler med utrymme för innovation:** den allmänna dataskyddsförordningen är teknologiskt neutral.

Det handlar om förtroende

Skydd av personuppgifter är en viktig angelägenhet för privatpersoner. De har därför lågt förtroende för digitala miljöer. Så här är det enligt en Eurobarometerundersökning:

- Åtta av tio personer känner att de inte har fullständig kontroll över sina personuppgifter.
- Sex av tio säger att de inte litar på företag på nätet.
- Över 90 procent av EU-invånarna säger att de vill ha samma dataskyddsnivå i samtliga EU-länder.

Den allmänna dataskyddsförordningen utgör ett nytt tillfälle för ditt företag att få upp konsumenternas förtroende genom riskbaserad personuppgiftshantering.

”Företag som inte klarar att skydda en privatpersons personuppgifter tillräckligt riskerar att tappa konsumentförtroende, något som är nödvändigt för att folk ska uppmuntras att använda nya produkter och tjänster.”

KAPITEL 2

ATT FÖRSTÅ DEN ALLMÄNNA DATASKYDDSFÖRORDNINGEN

Gäller den allmänna dataskyddsförordningen mig?

I det stora hela gäller den allmänna dataskyddsförordningen (GDPR) för ***varje*** företag som

behandlar personuppgifter genom **automatiserad** eller **manuell** behandling (förutsatt att uppgifterna ordnas enligt kriterier).

Även om ditt företag bara behandlar uppgifter på andra företags vägnar, så måste ni ändå rätta er efter reglerna.

Den allmänna dataskyddsförordningen gäller om

- ditt företag behandlar personuppgifter och är baserat i EU, oavsett var behandlingen av uppgifter faktiskt äger rum,
- ditt företag är etablerat utanför EU men erbjuder varor/tjänster till, eller övervakar beteendet hos, enskilda personer i EU.

Vad är personuppgifter?

Med personuppgifter menas all information som rör en identifierad eller identifierbar levande enskild person. Det kan innefatta

- namn,
- adress och telefonnummer,
- bostadsort,
- sjukjournaler,
- inkomst- och bankuppgifter,
- kulturella preferenser,
- med mera.

Personuppgifter som har avidentifierats, eller pseudonymiserats, men som ändå kan användas för att på nytt identifiera en person omfattas också av den allmänna dataskyddsförordningen. Personuppgifter som har gjorts oåterkalleligen anonyma på ett sådant sätt att personen inte längre går att identifiera anses emellertid inte som personuppgifter och styrs därför inte av den allmänna dataskyddsförordningen.

Förordningen är också teknologiskt neutral, vilket innebär att den skyddar personuppgifter oavsett vilken sorts teknik som används eller hur personuppgifterna lagras. Oavsett om ditt företag behandlar och lagrar personuppgifter med ett komplicerat IT-system eller i pappersarkiv, så styrs ni av den allmänna dataskyddsförordningen.

”Oavsett om ditt företag behandlar och lagrar personuppgifter med ett komplicerat IT-system eller I pappersarkiv, så styrs ni av den allmänna dataskyddsförordningen.”

Var extra försiktig med särskilda (känsliga) kategorier av personuppgifter

Om de personuppgifter ni samlar in innehåller information om en enskild persons hälsa, ras, sexuell läggning, religion, politiska uppfattning eller medlemskap i fackföreningar, så anses de vara känsliga. Ert företag får bara behandla dessa uppgifter under särskilda omständigheter, och ni kan behöva införa ytterligare skyddsåtgärder som t.ex. kryptering.

Vad innebär det att behandla personuppgifter?

Enligt den allmänna dataskyddsförordningen definieras åtgärder som att både samla in, använda och ta bort personuppgifter som behandling av personuppgifter.

Övervakar ni era lokaler via CCTV? Tittar ni i en databas med personuppgifter i affärssyften? Skickar ni reklam via e-post? Tar ni bort (digitala) mappar om anställda eller strimlar dokument? Eller lägger ni ut ett foto av en person på er webbplats eller era sociala mediekanaler?

Om ni svarade ja på något av detta, så behandlar ert företag helt klart personuppgifter.

Hur bidrar den allmänna dataskyddsförordningen till minskade kostnader?

Den allmänna dataskyddsförordningen tar hänsyn till företagens behov. Exempelvis har förordningen som syfte att få bort de administrativa kraven, för att minska kostnaderna och minimera den administrativa bördan.

- **Inga fler förhandsanmälningar:** Genom reformen avskaffas de flesta förhandsanmälningar till tillsynsmyndigheter, och därmed de kostnader som medföljde.
- **Dataskyddsombud:** Företagen behöver utnämna ett dataskyddsombud främst om deras kärnverksamhet innefattar behandling av känsliga uppgifter i stor omfattning, eller storskalig, regelbunden och systematisk övervakning av enskilda personer. Offentliga förvaltningar är skyldiga att utse ett dataskyddsombud.
- **Konsekvensbedömningar avseende dataskydd:** Företag måste utföra en konsekvensbedömning avseende dataskydd endast om en föreslagen databehandlingsverksamhet innebär en hög risk för enskilda personers rättigheter och friheter.
- **Registerföring:** Företag med färre än 250 anställda behöver inte föra register, utom när uppgiftsbehandlingen inte är tillfällig eller när den innehåller känslig information.

”Förordningen har som syfte att få bort de administrativa kraven, för att minska kostnaderna och minimera den administrativa bördan.”

KAPITEL 3

ERA SKYLDIGHETER ENLIGT DEN ALLMÄNNA DATASKYDDSFÖRORDNINGEN

Genom den allmänna dataskyddsförordningen (GDPR) åläggs vissa skyldigheter angående uppgiftsbehandling företag i hela EU. Enligt den allmänna dataskyddsförordningen får ett företag bara behandla personuppgifter enligt vissa villkor. Exempelvis bör behandlingen vara rättvis och öppen, den ska göras för ett angivet och berättigat ändamål, och vara begränsad till de uppgifter som behövs för att fullfölja det ändamålet. Den måste också bygga på en av följande rättsliga grunder:

- **Samtycke** från den berörda enskilda personen.
- En **avtalsenlig skyldighet** mellan er och den enskilda personen.
- Uppfyllande av en **rättslig förpliktelse**.
- Skydd av en enskild persons **grundläggande intressen**.
- Utförande av en **uppgift som är i det allmännas intresse**.
- Ert företags **berättigade intressen**, men först efter att ha kontrollerat att de grundläggande rättigheterna och friheterna för den person vars uppgifter ni behandlar inte påverkas allvarligt. Om personens rättigheter går före era intressen, så får ni inte behandla uppgifterna.

I fokus: att få samtycke till att använda personuppgifter

I den allmänna dataskyddsförordningen tillämpas stränga regler för att behandla uppgifter baserat på samtycke. Syftet med dessa regler är att säkerställa att den enskilda personen förstår vad det är han eller hon samtycker till. Detta innebär att samtycket ska vara **frivilligt**, **specifikt**, **informerat** och **otvetydigt**, genom en förfrågan som presenteras på ett klart och tydligt språk. Dessutom ska samtycke ges genom en **bekräftande handling**, som att markera en kryssruta online eller underteckna ett formulär.

Om ni behandlar personuppgifter som gäller ett **barn** baserat på samtycke, så krävs samtycke från förälder. Men eftersom åldersgränsen varierar mellan 13 och 16 år i olika länder, är det ett gott råd att ni ser efter i nationell lagstiftning.

Kom ihåg! När någon samtycker till behandling av sina personuppgifter, får ni bara behandla uppgifterna för de ändamål som samtycket lämnades för. Ni måste dessutom ge personen möjlighet att ta tillbaka samtycket.

Att fastställa er roll och ert ansvar

När du har dragit slutsatsen att den allmänna dataskyddsförordningen gäller för ditt företag och att det förekommer behandling av personuppgifter, så är nästa steg att fastställa er roll.

Dataskyddsreglerna skiljer mellan personuppgiftsansvarig och personuppgiftsbiträde, och olika skyldigheter gäller för var och en av dem. Medan den personuppgiftsansvarige avgör ändamålet med och metoderna för att samla in personuppgifterna, så behandlar personuppgiftsbiträdet uppgifter enbart på den personuppgiftsansvariges vägnar. Detta innebär dock inte att personuppgiftsbiträdet bara kan gömma sig bakom den personuppgiftsansvarige.

I den allmänna dataskyddsförordningen krävs att en personuppgiftsansvarig bara engagerar ett personuppgiftsbiträde som erbjuder tillräckliga garantier. Dessa garantier bör finnas med i ett skriftligt avtal mellan den personuppgiftsansvarige och personuppgiftsbiträdet. Avtalet måste också innehålla ett antal obligatoriska paragrafer, däribland t.ex. en paragraf som föreskriver att personuppgiftsbiträdet endast ska behandla personuppgifter enligt den personuppgiftsansvariges dokumenterade instruktioner.

Skyldigheter som skyddar den enskildes rättigheter

Den allmänna dataskyddsförordningen innehåller ett antal skyldigheter som syftar till att skydda en enskild persons rätt till kontroll över sina personuppgifter.

Er skyldighet: att lämna öppen information

Företag måste förse enskilda personer med information om vem som behandlar vad och varför. Som minst måste det tydligt anges i denna information

- vilka ni är,
- varför ni behandlar uppgifterna,
- vilken den rättsliga grunden är,
- vem som kommer att få uppgifterna (i tillämpliga fall).

I vissa fall måste det i informationen också uppges

- kontaktinformation till dataskyddsombudet,
- vad det berättigade intresset är (när berättigat intresse är den rättsliga grunden för behandling),
- grunden för att överföra uppgifterna till ett land utanför EU,
- hur länge uppgifterna kommer att lagras,
- den enskilda personens dataskyddsrättigheter (d.v.s. rätt att få tillgång, korrigera, radera, begränsa, invända, rätt till portabilitet osv.),
- hur samtycke kan tas tillbaka (när samtycke är den rättsliga grunden för behandling),
- om det finns en lagstadgad skyldighet eller avtalsförpliktelse att lämna uppgifterna,
- när det gäller automatiserat beslutsfattande information om logiken bakom beslutet, dess betydelse och konsekvenser.

”Företag måste förse enskilda personer med information om vem som behandlar vad och varför.”

Er skyldighet: rätt att få tillgång och rätt till dataportabilitet

Enskilda personer har rätt att begära tillgång till sina personuppgifter, kostnadsfritt och i ett tillgängligt format. Om ni får en sådan begäran måste ni

- tala om för personen om ni behandlar hans/hennes personuppgifter,
- informera personen om behandlingen (såsom ändamålen med behandlingen, berörda kategorier av personuppgifter, mottagare av personens uppgifter osv.),
- tillhandahålla en kopia av de personuppgifter som behandlas.

När behandlingen grundar sig på samtycke eller ett avtal, kan dessutom den enskilda personen be att hans/hennes personuppgifter återlämnas eller överförs till ett annat företag. Detta kallas för rätten till dataportabilitet. Uppgifterna bör tillhandahållas i ett vanligt använt och maskinläsbart format.

Även om dessa två rättigheter har nära samband med varandra, så är de ändå två olika rättigheter. Ni måste därför se till att de två rättigheterna inte förväxlas, och upplysa den enskilda personen därefter.

Er skyldighet: rätt till radering (rätten att bli bortglömd)

Under vissa omständigheter kan en enskild person begära att den personuppgiftsansvarige raderar hans eller hennes personuppgifter, t.ex. när uppgifterna inte längre behövs för att uppfylla ändamålet med behandlingen. Ditt företag är dock inte skyldigt att följa en sådan begäran från en enskild person om

- behandlingen är nödvändig för att respektera någons yttrande- och informationsfrihet,
- ni måste behålla personuppgifterna för att uppfylla en rättslig skyldighet,
- det finns andra skäl av allmänt intresse för att behålla personuppgifterna, t.ex. folkhälsa eller vetenskapliga och historiska forskningsändamål,
- ni behöver behålla personuppgifterna för att göra ett rättsligt anspråk.

Er skyldighet: rätt att korrigera och rätt att invända

Om en enskild person anser att hans eller hennes personuppgifter är inkorrekta, ofullständiga eller felaktiga, så har han eller hon rätt att få dem rättade eller kompletterade utan onödigt dröjsmål.

En enskild person kan också när som helst invända mot att hans/hennes personuppgifter behandlas i ett visst syfte när ditt företag behandlar dem grundat på ert berättigade intresse eller för att utföra en uppgift av allmänt intresse. Om ni inte har ett berättigat intresse som går före den enskilda personens intresse, måste ni sluta behandla personuppgifterna. På samma sätt kan en enskild person be att få behandlingen av sina personuppgifter begränsad medan det avgörs om ert berättigade intresse går före personens intresse eller inte. När det gäller direkt marknadsföring är ni emellertid alltid skyldiga att sluta behandla personuppgifterna på den enskilda personens begäran.

En förmaning angående automatiserat beslutsfattande och profilering

Enskilda personer har rätt att inte underställas ett beslut som enbart är baserat på automatiserad behandling. Det finns dock vissa undantag från denna regel, som när personen uttryckligen har samtyckt till det automatiserade beslutet. Förutom när det automatiserade beslutet är baserat på en lag, måste ert företag

- informera den enskilda personen om det automatiserade beslutsfattandet,
- ge personen rätt att få det automatiserade beslutet granskat av en riktig person,
- ge personen möjlighet att bestrida det automatiserade beslutet.

Om till exempel en bank automatiserar sitt beslut angående om ett lån ska beviljas en viss enskild person eller inte, så bör den enskilda personen informeras om det automatiserade beslutet och ges möjlighet att bestrida beslutet och begära ett mänskligt ingripande.

Skyldigheter grundade på risk

Förutom de skyldigheter som syftar till att skydda individuella rättigheter, innehåller den allmänna dataskyddsförordningen också ett antal skyldigheter vars tillämpning beror på risken.

Er skyldighet: att utse ett dataskyddsombud

Ett dataskyddsombud ansvarar för att övervaka er efterlevnad av den allmänna dataskyddsförordningen. En av dataskyddsombudets huvuduppgifter är att informera och ge råd till de anställda som faktiskt behandlar personuppgifterna om deras skyldigheter. Dataskyddsombudet samarbetar också med dataskyddsmyndigheten och fungerar som kontaktpunkt gentemot dataskyddsmyndigheten och enskilda personer.

Ert företag måste utse ett dataskyddsombud när

- ni regelbundet eller systematiskt övervakar enskilda personer eller behandlar särskilda kategorier av uppgifter,
- denna behandling är en grundläggande affärsverksamhet,
- ni gör det i stor omfattning.

Om ni exempelvis behandlar personuppgifter för att ge målinriktad reklam genom sökmotorer baserat på folks beteende på nätet, så kräver den allmänna dataskyddsförordningen att ni har ett dataskyddsombud. Om ni emellertid bara skickar reklammaterial till era kunder en gång om året, så behövs inget dataskyddsombud. Om du är läkare som samlar in uppgifter om patienternas hälsa, så behövs det på samma sätt förmodligen inget dataskyddsombud. Men om du behandlar personuppgifter om genetik och hälsa åt ett sjukhus, så behövs det ett dataskyddsombud.

Er skyldighet: inbyggt dataskydd och dataskydd som standard

Genom den allmänna dataskyddsförordningen införs två nya principer: inbyggt dataskydd och dataskydd som standard.

Inbyggt dataskydd hjälper till att se till att ett företag tar hänsyn till dataskyddet i de tidiga stadierna när de planerar ett nytt sätt att behandla personuppgifter. I enlighet med denna princip måste en personuppgiftsansvarig vidta alla tekniska och organisatoriska mått och steg som behövs för att införa dataskyddsprinciperna och skydda enskilda personers rättigheter. Dessa steg kan exempelvis innefatta att använda pseudonymisering.

Inbyggt dataskydd minimerar integritetsriskerna och ökar förtroendet. Genom att sätta dataskyddet i första rummet redan när nya varor eller tjänster utvecklas, så kan eventuella dataskyddsproblem undvikas i ett tidigt skede. Denna rutin hjälper också till att höja medvetenheten om dataskydd på alla avdelningar och nivåer i ett företag.

Dataskydd som standard innebär att ni ser till att ert företag alltid gör den mest integritetsvänliga miljön till standardmiljö. Om t.ex. två integritetsmiljöer är möjliga och en av miljöerna förhindrar att andra får åtkomst till personuppgifter, så bör den användas som standardmiljö.

”Inbyggt dataskydd minimerar integritetsriskerna och ökar förtroendet.”

”Dataskydd som standard innebär att ni ser till att ert företag alltid gör den mest integritetsvänliga miljön till standardmiljö.”

Er skyldighet: att anmäla ordentligt i händelse av en personuppgiftsincident

En personuppgiftsincident inträffar när de personuppgifter som ni ansvarar för avslöjas, antingen oavsiktligt eller olagligt, för obehöriga mottagare eller görs tillfälligt otillgängliga eller ändras.

Det är mycket viktigt att ett företag inför lämpliga tekniska och organisatoriska åtgärder för att undvika personuppgiftsincidenter. Om en personuppgiftsincident ändå inträffar och incidenten utgör en risk för enskilda personers rättigheter och friheter, bör ni meddela er dataskyddsmyndighet inom 72 timmar efter att ni blev medvetna om incidenten.

Beroende på om personuppgiftsincidenten utgör en hög risk för de berörda eller inte, så kan ett företag också behöva informera alla enskilda personer som berörs av personuppgiftsincidenten.

Överföra personuppgifter utanför EU?

Den allmänna dataskyddsförordningen gäller för det europeiska ekonomiska samarbetsområdet (EES), som innefattar samtliga EU-länder plus Island, Liechtenstein och Norge. När personuppgifter överförs utanför EES, bör de skydd som den allmänna dataskyddsförordningen ger medfölja uppgifterna. Det innebär att företag för att exportera uppgifter utomlands måste se till att vissa skyddsåtgärder finns.

I den allmänna dataskyddsförordningen finns en rik uppsättning av olika mekanismer för att överföra uppgifter till tredjeländer. Enligt förordningen är sådana överföringar tillåtna när

1. landets skydd bedöms som adekvata av EU,
2. ert företag exempelvis vidtar de nödvändiga åtgärderna för att tillhandahålla lämpliga skydd, såsom att ta med särskilda paragrafer i det avtal som ingås med den icke-europeiska importören av personuppgifterna,
3. ert företag exempelvis förlitar sig på särskilda grunder för överföringen (kallade ”undantag”) som t.ex. den enskilda personens samtycke.

För mer information om de regler som gäller för internationella uppgiftsöverföringar, se Europeiska kommissionens meddelande om utbyte och skydd av personuppgifter i en globaliserad värld: http://eur-lex.europa.eu/legal-content/SV/TXT/HTML/?uri=CELEX:52017DC0007&from=SV

Måste ni göra en konsekvensbedömning avseende dataskydd?

Det är obligatoriskt att utföra en konsekvensbedömning avseende dataskydd varje gång den avsedda behandlingen skulle kunna leda till att enskilda personers rättigheter och friheter utsätts för hög risk. Så kan exempelvis vara fallet när nya tekniktyper används.

Enligt den allmänna dataskyddsförordningen föreligger sådan hög risk åtminstone när

- automatiserade behandlings- och profileringsmekanismer används för att systematiskt och omfattande bedöma enskilda personer,
- ett offentligt tillgängligt område övervakas systematiskt i stor omfattning (t.ex. CCTV),
- känsliga uppgifter behandlas i stor skala (t.ex. hälsouppgifter).

Syftet med konsekvensbedömningen avseende dataskydd är att identifiera potentiella risker för enskilda personers rättigheter och friheter innan behandlingen av personuppgifter börjar och innan risken uppkommer. Genom att minska risken på förhand kan skador undvikas och kostnader minimeras.

Om alla de identifierade höga riskerna inte avhjälps genom de åtgärder som anges i konsekvensbedömningen, så måste dataskyddsmyndigheten rådfrågas innan den avsedda uppgiftsbehandlingen äger rum.

”Det är obligatoriskt att utföra en konsekvensbedömning avseende dataskydd varje gång den avsedda behandlingen skulle kunna leda till att enskilda personers rättigheter och friheter utsätts för hög risk.”

Vad ni behöver göra

Svara på begäranden

Om ditt företag får en begäran från en enskild person som vill utöva sina rättigheter, så bör ni svara på denna begäran utan onödigt dröjsmål och alltid inom en månad från att ni mottog begäran. Denna svarstid kan dock förlängas med två månader vid komplicerade ärenden eller många begäranden samtidigt, så länge personen informeras om förlängningen. Begäranden bör också handläggas **kostnadsfritt**. Om en begäran avvisas, måste ni informera personen om skälen till detta och om hans/hennes rätt att lämna in ett klagomål hos dataskyddsmyndigheten.

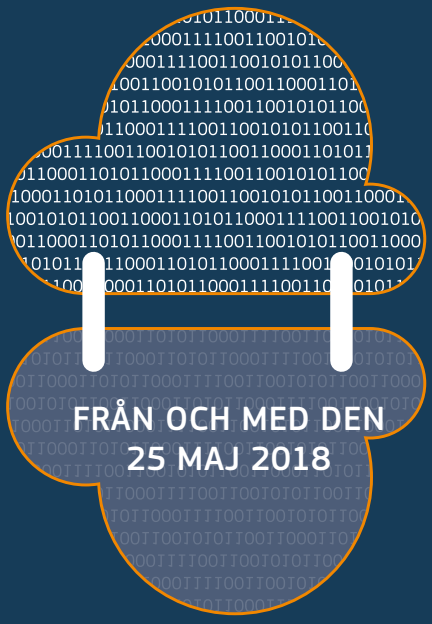
Uppvisa efterlevnad och för register!

En av grundprinciperna bakom den allmänna dataskyddsförordningen är att säkerställa att företagen kan uppvisa efterlevnad. Detta innebär att ni måste kunna bevisa att ert företag handlar i enlighet med den allmänna dataskyddsförordningen och uppfyller alla tillämpliga skyldigheter – i synnerhet på begäran av dataskyddsmyndigheten eller vid inspektion från den.

Ett sätt att göra detta är att föra detaljerade register över sådant som

- namn och kontaktuppgifter till ert företag som sysslar med behandling av uppgifter,
- skäl till att behandla personuppgifter,
- beskrivning av de kategorier av enskilda personer som lämnar personuppgifter,
- kategorier av organisationer som får personuppgifterna,
- överföring av uppgifter till ett annat land eller annan organisation,
- lagringstid för personuppgifterna,
- beskrivning av säkerhetsåtgärder som används vid behandling av personuppgifter.

Dessutom bör ert företag också upprätthålla – och regelbundet uppdatera – skriftliga rutiner och riktlinjer och se till att era anställda känner till dem.



KAPITEL 4

REDO ATT GÖRA RÄTT?

När det gäller att behandla personuppgifter medför den allmänna dataskyddsförordningen (GDPR) att bollen ligger hos er. Första steget är att kartlägga er nuvarande uppgiftsbehandlingsverksamhet och på nytt utvärdera era interna affärsprocesser. I synnerhet måste ni

- identifiera vilka uppgifter ni innehar och för vilket ändamål, och på vilken rättslig grund ni innehar dem,
- bedöma alla avtal som finns, i synnerhet de mellan personuppgiftsansvariga och personuppgiftsbiträden,
- bedöma alla tillgängliga vägar för internationella överföringar,
- gå igenom förvaltningen av ert företag i allmänhet (d.v.s. vad för slags IT och organisatoriska åtgärder ni har inrättade), däribland om ni måste eller vill utnämna ett dataskyddsombud.

En nödvändig del av denna process är att se till att ert företags högsta ledningsnivå är involverad i sådana genomgångar, och ger synpunkter och hålls regelbundet uppdaterade och rådfrågas om ändringar av personuppgiftspolicyn.

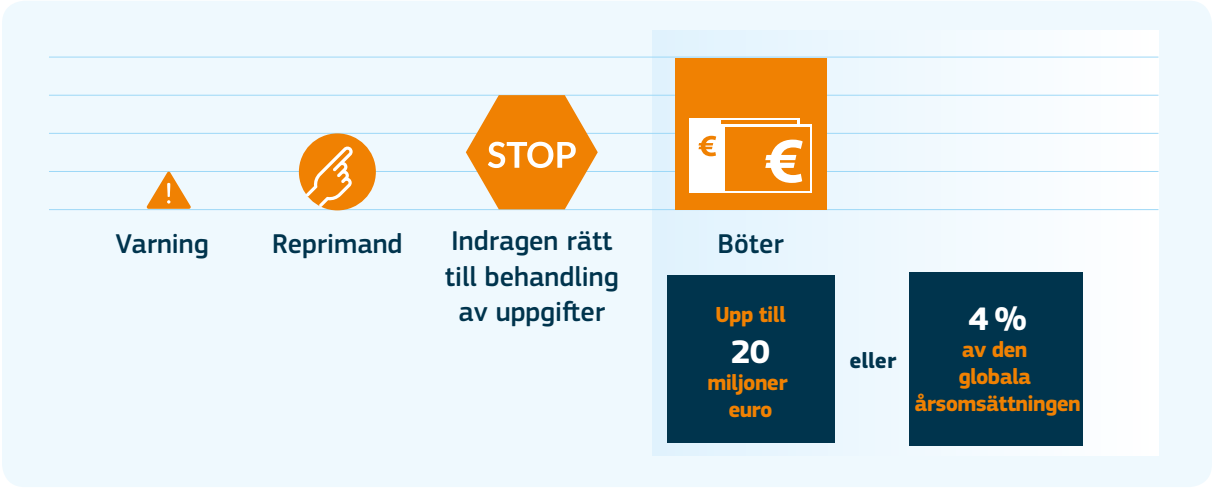
Behandlar ni uppgifter i fler än ett land?

Vid gränsöverskridande behandling kan det vara en tillsynsmyndighet i ett annat land, och inte er nationella dataskyddsmyndighet, som är den behöriga myndigheten. Normalt rör det sig om dataskyddsmyndigheten i det land som står värd för ert företags huvudsakliga verksamhetsställe (där besluten om metoderna för och ändamålen med behandling fattas) inom EU.

Riskerna med avvikelser

Att inte följa den allmänna dataskyddsförordningen kan leda till betydande böter – för vissa överträdelser upp till 20 miljoner euro eller 4 procent av ert företags globala omsättning. Dataskyddsmyndigheten kan ålägga ytterligare korrigerande åtgärder, som att beordra att behandlingen av personuppgifter upphör. Ni bör också tänka på det dåliga rykte som dålig efterlevnad kan orsaka.

Kostnaderna för att inte följa den allmänna dataskyddsförordningen är helt klart mycket större än eventuella investeringar för att följa den.



Frågor? Funderingar? Vänd dig till din nationella dataskyddsmyndighet.

Hitta din nationella dataskyddsmyndighet online

http://ec.europa.eu/justice/data-protection/article-29/structure/data-protection-authorities/index_en.htm

VIKTIGT MEDDELANDE

Syftet med informationen och vägledningen i denna broschyr är att bidra till en bättre uppfattning om EU:s dataskyddsregler.

Detta är enbart menat som ett vägledande verktyg – endast texten i den allmänna dataskyddsförordningen 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 broschyren kan komma att användas.

Denna broschyr speglar situationen när den författades och ska ses som ett ”levande dokument” som är öppet för förbättringar, och dess innehåll kan komma att ändras utan förvarning.

Kontakta EU

Besök

Det finns hundratals Europa direkt-kontor i hela EU. Hitta ditt närmaste kontor på https://europa.eu/european-union/contact_sv.

Telefon eller mejl

Tjänsten Europa direkt svarar på dina frågor om EU. Kontakta tjänsten på något av följande sätt:
– Ring det avgiftsfria telefonnumret 00 800 6 7 8 9 10 11 (en del operatörer kan ta betalt för samtalet).
– Ring telefonnumret +32 22999696.
– Mejla via webbplatsen (https://europa.eu/european-union/contact_sv).

EU-information

På nätet

På webbplatsen Europa finns det information om EU på alla officiella EU-språk (https://europa.eu/european-union/index_sv).

EU-publikationer

Ladda ned eller beställ både gratis och avgiftsbelagda EU-publikationer från EU Bookshop (https://publications.europa.eu/bookshop). Om du behöver flera kopior av en gratispublikation kan du kontakta Europa direkt eller ditt lokala informationskontor (https://europa.eu/european-union/contact_sv).

EU-lagstiftning och andra rättsliga handlingar

Rättsliga handlingar från EU, inklusive all EU-lagstiftning sedan 1952, finns på alla officiella EU-språk på EUR-Lex (http://eur-lex.europa.eu).

Öppna data från EU

På EU:s portal för öppna data (http://data.europa.eu/euodp/sv) finns dataserier från EU. Dataserierna får laddas ned och användas fritt för kommersiella och andra ändamål.

DS-01-18-082-SV-C

Den allmänna dataskyddsförordningen (GDPR) reglerar hur företag behandlar och hanterar personuppgifter. Med en enda europeisk lag för skydd av personuppgifter behöver nu ditt företag i första hand anpassa sig till en dataskyddslagstiftning när det erbjuder varor och tjänster någonstans i EU.

Genom att den allmänna dataskyddsförordningen förenklar regelverket för företag, utgör den en ny möjlighet för ditt företag att förbättra personuppgiftshanteringen och därmed höja konsumenternas förtroende för företaget.

I den här broschyren betonas de skyldigheter ditt företag har enligt den allmänna dataskyddsförordningen.

europa.eu/dataprotection/sv

Publikationsbyrån

ISBN 978-92-79-79454-4