



Building a better  
working world

## Reglerna och föreskrifterna gällande dataskyddsfrågor preciseras

Genom EU:s allmänna dataskyddsförordning (GDPR), som fastställdes 2016 och trädde i kraft 2018, har dataskyddsfrågor blivit en allt större del av företagens vardag. Förutom dataskyddsförordningen och dess inverkan på den nationella dataskyddslagen, har även mer detaljerade riktlinjer och tolkningar utfärdats under 2020, bland annat av dataombudsmannen och EU-domstolen. Riktlinjerna har bland annat avsett företagens tillvägagångssätt gällande dataskydd, överföringen av uppgifter mellan EU och USA samt användningen av kakor på företagens webbplatser. De första sanktionerna för dataskyddsöverträdelser

i Finland har även utdömts. Det är således hög tid för företagen att se till att deras tillvägagångssätt och dokumentation gällande dataskydd är uppdaterade och lagenliga.





## De första påföljdsavgifterna i Finland har utdömts

Påföljdskollegiet vid dataombudsmannens byrå utdömde i maj 2020 de första påföljdsavgifterna till fyra företag som har gjort sig skyldiga till dataskyddsöverträdelser. En femte påföljdsavgift utdömdes även i augusti 2020. En av påföljdsavgifterna som utdömdes berodde på brister i de lagstadgade informationsskyldigheterna. Företaget i fråga hade bland annat inte informerat sina kunder om rätten att vägra att deras personuppgifter lämnas vidare. Detta resulterade i att kunderna blev föremål för direktmarknadsföring och kontaktade av andra företag. Totalt drabbades 161 000 kunder av dataskyddsöverträdelserna och företaget i fråga påfördes en påföljdsavgift om 100 000 euro. Företag bör således vara särskilt uppmärksamma på hur de registrerade, till exempel kunder, informeras om behandlingen och överföringen av deras personuppgifter. De lagstadgade kraven avseende dessa delar är tämligen strikta.

Under vissa förutsättningar är företag skyldiga enligt dataskyddslagen att bedöma inverkan av en personuppgiftsbehandling. Vid en sådan konsekvensbedömning ska man bedöma behovet av åtgärderna, om åtgärderna står i rätt proportion samt därtill hörande risker med behandlingen. För två bolag ledde bristen på en sådan konsekvensbedömning till påföljdsavgifter. Ett av företagen som fick en påföljdsavgift hade behandlat sina arbetstagares positionsuppgifter. Företaget hade lokaliserat arbetstagarnas fordon för att övervaka deras arbetstider. Fallet ledde till en påföljdsavgift om 16 000 euro. Det andra företaget, som också hade samlat in positionsinformation, hade använt säkerhetskameraövervakning och spelat in ljud i taxibilar, utan att berätta om detta för kunderna. Taxibolaget hade även flera brister i sin informationspraxis och dokumentation samt i definitionerna av rollerna vid behandling av personuppgifter. Påföljdsavgiften i detta fall var 72 000 euro. Till exempel vid frågor gällande kameraövervakning kan en särskild omsorg förutsättas av företagen, även om det endast handlar om övervakning av säkerheten i en lokal.

Ett väsentligt krav vid behandling av personuppgifter är att företagen ska kunna motivera behovet av behandlingen från fall till fall. Om uppgifter behandlas, till exempel om en arbetstagares religiösa övertygelse eller annan information som kan anses vara onödig, kan denna onödiga behandling resultera i sanktioner. Påföljdskollegiet vid dataombudsmannens byrå har utdömt en påföljdsavgift om 12 500 euro till ett företag som behandlade onödig informationen om anställda och potentiella anställda under rekryteringsfasen.

Den senaste påföljdsavgiften, som utdömdes i augusti, gällde direktmarknadsföringsmeddelanden som ett företag hade skickat till sina kunder utan att ha erhållit kundens på förhand givna godkännande. Påföljdsavgiften som utdömdes i detta fall var 7 000 euro. Företag måste med andra ord också vara särskilt uppmärksamma på åtgärder som kan hänföras till direktmarknadsföring.

De utdömda påföljdsavgifterna är ett tydligt tecken på att dataskyddsmyndigheten har tagit dataskyddsöverträdelser på allvar och att myndigheten blivit allt mer aktiv inom tillsyn och tolkning av lagstiftningen även i Finland. I Europa har dataskyddsmyndigheterna i olika länder redan tidigare utdömt betydligt högre sanktioner.

## Myndigheternas föreskrifter gällande kakor har preciserats

Kakor (cookies) är ett allmänt använt och behändigt sätt att samla in information om bland annat besökarens beteende på webbplatsen. Detta möjliggör riktad information och reklam till besökaren som faller inom just den personens preferenser. Användningen av kakor förutsätter samtycke från personer som besöker webbplatsen. Samtycket måste enligt dataskyddsförordningen vara en frivillig, individualiserad, informativ och entydig viljeförklaring, genom vilken personen godkänner behandlingen av personuppgifter. Tidigare har det varit vanligt med en slags anmälan, en så kallad banner, som till exempel säger "Genom att fortsätta använda webbplatsen godkänner du användningen av kakor" eller "Genom att trycka på OK-knappen, godkänner du alla kakor".

Den biträdande datatillsynsmannen tog ställning till sådana anmälningar i sitt beslut 14.5.2020 och yttrade att motsvarande metoder för att samla in samtycke inte uppfyller villkoren för ett giltigt samtycke enligt dataskyddsförordningen. Användaren ges inte möjlighet att självständigt välja om han ska acceptera eller avvisa användningen av kakor. I stället bör användaren vara helt fri att godkänna användningen av cookies genom sin egen aktiva handling, till exempel genom att själv kryssa för rutan "OK" eller genom att välja "Jag godkänner" -knappen i stället för "Avvisa" -knappen. Utöver dessa villkor bör det säkerställas att ett återtagande av samtycke är precis lika enkelt som att ge det, samt att den så kallade bannern som samlar in samtycket inte stör användningen av webbplatsen.

Den biträdande datatillsynsmannens beslut klargör den tidigare, något ospecificerade rättsliga situationen och skyddar personer från insamling av personuppgifter till följd av deras ovetskap eller oavsiktlighet. Varje företag bör nu utvärdera kakor-praxis och tillhörande meddelanden på sin webbplats och vid behov uppdatera dessa.

## Dataskydd och coronaviruset

Som ett resultat av coronaviruset kan arbetsgivare ha efterfrågat och bokfört arbetstagares hälsotillstånd och familjeomständigheter mer än vanligt. Arbetsgivare och personer som behandlar personuppgifterna måste fortfarande komma ihåg att behandla arbetstagares hälsouppgifter konfidentiellt, proportionerligt och skäligt enligt lag. Detta krav anges också starkt i den för arbetsgivarna bindande lagen om integritetsskydd i arbetslivet. Detta innebär till exempel att arbetsgivaren eller den som behandlar hälsouppgifterna alltid har tystnadsplikt och att arbetsgivaren som utgångspunkt inte får namnge den person som lider av corona på något identifierbart sätt.

En arbetsgivare kan inte som utgångspunkt tvinga en arbetstagare att genomgå ett coronatest, men arbetsgivare har rätt att hindra en person från att arbeta om arbetsgivaren misstänker att arbetstagaren har smittats av coronaviruset. En arbetstagare kan godkänna behandling, insamling och överlåtelse av sina hälsouppgifter, men i sådana fall måste samtycket uppfylla ovannämnda krav i dataskyddsförordningen för att vara giltigt.

## Privacy Shield-regleringen gällande USA upphörde att gälla i juli

Den så kallade Privacy Shield-regleringen har skapat en utgångspunkt för överföring av information mellan EU och USA som krävs enligt dataskyddslagstiftningen. Syftet har bland annat varit att skydda bolag som är verksamma inom EU från att de amerikanska myndigheterna ska ha tillgång till personuppgifterna. I juli 2020 konstaterade EU-domstolen i sitt så kallade Schrems II-beslut, att genom ikraftträdandet av EU:s dataskyddsförordning, uppfyller Privacy Shield-regleringen inte längre EU:s dataskyddsstandarder. På grund av detta ligger inte heller säkerhet och dataskydd vid behandling av personuppgifter i USA på en tillräcklig nivå. Mot bakgrund av dessa premisser upphävde EU-domstolen Privacy Shield-regleringen.

Det är enkelt att tänka att detta beslut inte berör ditt företag, men så är tyvärr inte fallet. EU-domstolens avgörande berör ett stort antal aktörer, då flera företag använder tjänsteleverantörer som verkar inom Privacy Shield-regleringen. Till exempel kan många allmänna företag, bland annat sådana som erbjuder tjänster inom marknadsföring, ha sitt huvudkontor i USA och informationen har då överlämnats till USA genom Privacy Shield-regleringen. Det är därför nu upp till företagen att se till att dessa tjänsteleverantörer kan garantera en laglig och säker överföring av personuppgifter genom att använda andra skyddsåtgärder som krävs enligt lag. Det rekommenderas därför att företag granskar alla sina avtal om behandling av personuppgifter. Företag bör kontrollera om avtalen ger den registeransvarige rätten att behandla uppgifter i länder utanför EU/EES, och i så fall under vilka villkor och på vilket sätt det bör förverkligas.

EY ger gärna ytterligare information om linjedragningar i dataskyddsärenden och hjälper er med frågor gällande dataskydd.

## EY | Assurance | Tax | Strategy and Transactions | Consulting

### Om EY

EY är ett världsledande företag inom revision, redovisning, skatt, transaktioner och affärsrådgivning. Våra tjänster och insikter hjälper till att skapa förtroende och hållbar tillväxt på finansmarknader och i ekonomier världen över. För att hålla våra löften till våra intressenter utvecklar vi ledare och medarbetare som arbetar i team över gränserna. Vi vill att allt vi gör ska bidra till att affärsvärlden och arbetslivet fungerar bättre - för våra medarbetare, våra kunder och de samhällen vi verkar i. Läs mer på vår webbsida [www.ey.com/fi/](http://www.ey.com/fi/) och följ oss på Twitter @EY\_Suomi.

© 2020 Ernst & Young AB

All rights reserved.

## Kontakta oss



### Joe Gummerus

Senior Legal Counsel  
p. +358 40 350 7334  
[joe.gummerus@fi.ey.com](mailto:joe.gummerus@fi.ey.com)



### Mira Ahonen

Associate Legal Counsel  
p. +358 44 268 1826  
[mira.ahonen@fi.ey.com](mailto:mira.ahonen@fi.ey.com)

[www.ey.com/fi](http://www.ey.com/fi)