

WP 244 BILAGA II – VANLIGA FRÅGOR OCH SVAR

Vad är en ansvarig tillsynsmyndighet?

Enligt den allmänna dataskyddsförordningen är den generella regeln att endast en tillsynsmyndighet, som kallas den ansvariga tillsynsmyndigheten, leder tillsynen av gränsöverskridande behandling eller behandling som rör medborgare från mer än ett EU-land, enligt principen om en enda kontaktpunkt.

Den ansvariga tillsynsmyndigheten är den myndighet som har det främsta ansvaret för att övervaka *gränsöverskridande behandling*, till exempel vid utredningar av företag som genomför behandling i flera medlemsstater.

Den ansvariga tillsynsmyndigheten samordnar insatser som rör de berörda tillsynsmyndigheterna enligt artiklarna 60–62 i förordningen (t.ex. en enda kontaktpunkt, ömsesidigt bistånd och gemensamma insatser). Den lägger fram utkast till beslut inför de tillsynsmyndigheter som berörs av ärendet.

Vad är gränsöverskridande behandling?

Ansvariga tillsynsmyndigheter utses endast i samband med gränsöverskridande behandling. Därför måste det fastställas om gränsöverskridande behandling äger rum.

Enligt artikel 4.23 i förordningen innebär gränsöverskridande behandling antingen

- behandling av personuppgifter som äger rum inom ramen för verksamhet vid verksamhetsställen i mer än en medlemsstat tillhörande en personuppgiftsansvarig eller ett personuppgiftsbiträde i unionen, när den personuppgiftsansvarige eller personuppgiftsbiträdet är etablerad i mer än en medlemsstat, eller
- behandling av personuppgifter som äger rum inom ramen för verksamhet vid ett enda verksamhetsställe tillhörande en personuppgiftsansvarig eller ett personuppgiftsbiträde i unionen men som i väsentlig grad påverkar eller sannolikt i väsentlig grad kommer att påverka registrerade i mer än en medlemsstat.

Vad betyder ”påverka i väsentlig grad”?

Detta definieras inte i förordningen.

Tillsynsmyndigheterna tolkar begreppet ”påverka i väsentlig grad” från fall till fall. De faktorer som övervägs inom ramen för behandlingen är typen av uppgifter, ändamålet med behandlingen och om behandlingen

- orsakar eller sannolikt kan orsaka skada, förlust eller känslomässigt lidande för enskilda personer,
- har, eller sannolikt kan ha, en faktisk påverkan genom att den enskilda personens rättigheter begränsas eller han/hon förlorar en möjlighet,
- påverkar, eller sannolikt kan påverka, den enskilda personens hälsa, välbefinnande eller trygghet,
- påverkar, eller sannolikt kan påverka, den enskilda personens finansiella eller ekonomiska ställning eller situation,
- utsätter den enskilda personen för diskriminering eller orättvis behandling,

- omfattar analys av särskilda kategorier av personuppgifter eller andra inkräktande uppgifter, särskilt barns personuppgifter,
- leder till, eller sannolikt kan leda till att den enskilda personen ändrar sitt beteende på ett väsentligt sätt,
- leder till osannolika, oväntade eller oönskade konsekvenser för den enskilda personen,
- ger upphov till pinsamma situationer eller andra negativa resultat, även skadat anseende, eller
- innebär behandling av en stor mängd personuppgifter.

Hur fastställs den personuppgiftsansvariges ansvariga tillsynsmyndighet?

När det har konstaterats att behandlingen är gränsöverskridande måste man fastställa vilken tillsynsmyndighet som är ansvarig.

Enligt artikel 56 i förordningen ska tillsynsmyndigheten i det land där organisationen har sitt huvudsakliga verksamhetsställe vara ansvarig tillsynsmyndighet.

Om organisationen har sitt enda verksamhetsställe i EU, men behandlingen i väsentlig grad påverkar eller sannolikt i väsentlig grad kommer att påverka registrerade i mer än en medlemsstat, är det tillsynsmyndigheten där det enda verksamhetsstället finns som är ansvarig.

Om organisationen har flera verksamhetsställen i EU är principen att det huvudsakliga verksamhetsstället är platsen för organisationens centrala förvaltning. Om ett annat verksamhetsställe fattar besluten om ändamålen och medlen för behandlingen, och har befogenhet att få sådana beslut genomförda, är detta verksamhetsställe det huvudsakliga verksamhetsstället. Det är de personuppgiftsansvarigas uppgift att tydligt fastställa var besluten om ändamålen och medlen för behandlingen av personuppgifter fattas.

Ett exempel: Om ett företag har en eller flera verksamhetsformer som omfattar gränsöverskridande behandling och besluten om all gränsöverskridande behandling fattas inom EU, som alltså är platsen för företagets centrala förvaltning, utses en enda ansvarig tillsynsmyndighet för all gränsöverskridande behandling. Det är tillsynsmyndigheten på platsen för företagets centrala förvaltning som är ansvarig tillsynsmyndighet.

Om ett företag emellertid har flera verksamhetsformer som omfattar gränsöverskridande behandling och besluten om ändamålet och medlen för behandlingen fattas vid andra verksamhetsställen, utses fler än en ansvarig tillsynsmyndighet. Då är det tillsynsmyndigheterna på platserna för de verksamhetsställen som fattar besluten om respektive gränsöverskridande behandling som är ansvariga tillsynsmyndigheter. För att fullständigt dra nytta av principen om en enda kontaktpunkt, dvs. att det endast ska finnas en enda ansvarig tillsynsmyndighet för all gränsöverskridande behandling, bör företagen överväga att förlägga beslutsbefogenheterna för behandling av personuppgifter till ett enda verksamhetsställe.

Vilka kriterier används för att fastställa den personuppgiftsansvariges ansvariga tillsynsmyndighet?

Nedanstående frågor är till hjälp för att fastställa platsen för personuppgiftsansvarigas huvudsakliga verksamhetsställe:

- Har den personuppgiftsansvarige ett enda verksamhetsställe i EU?

Om så är fallet, och om behandlingen i väsentlig grad påverkar eller sannolikt i väsentlig grad kommer att påverka de registrerade i mer än en medlemsstat, är det tillsynsmyndigheten där det enda verksamhetsstället finns som är ansvarig.

- Har den personuppgiftsansvarige ett huvudkontor i EU?
 - Om så är fallet, vilken roll har huvudkontoret? Fattas besluten om ändamålen och medlen för behandlingen inom detta verksamhetsställe och har det befogenheten att genomföra beslut om behandling?
 - Om så inte är fallet, finns det andra verksamhetsställen
 - där man fattar beslut om affärsverksamhet som omfattar behandling av personuppgifter?
 - som har den faktiska befogenheten att genomföra beslut?
 - där direktören (eller direktörerna) som har det huvudsakliga ansvaret för den gränsöverskridande behandlingen finns?
 - där den personuppgiftsansvarige eller personuppgiftsbiträdet är registrerad som ett företag, om behandlingen sker inom ett enda territorium?

Hur fastställs personuppgiftsbitrådets ansvariga tillsynsmyndighet?

Enligt förordningen får även personuppgiftsbiträden som omfattas av förordningen och har verksamhetsställen i mer än en medlemsstat utnyttja systemet med en enda kontaktpunkt.

Enligt artikel 4.16 b ska personuppgiftsbitrådets verksamhetsställe vara den plats i EU där personuppgiftsbiträdet har sin centrala förvaltning eller, om personuppgiftsbiträdet inte har någon central förvaltning i EU, det av personuppgiftsbitrådets verksamhetsställen i EU där den huvudsakliga behandlingen sker.

Enligt skäl 36 ska dock den personuppgiftsansvariges tillsynsmyndighet vara ansvarig tillsynsmyndighet i fall som omfattar både en personuppgiftsansvarig och ett personuppgiftsbiträde. I denna situation anses personuppgiftsbitrådets tillsynsmyndighet vara en "berörd tillsynsmyndighet", och bör delta i samarbetsförfarandet.