Ram för dataskydd mellan EU och USA

SVAR PÅ VANLIGA FRÅGOR FÖR EUROPEISKA FÖRETAG[1]

Antaget den 16 juli 2024

Translations proofread by EDPB Members.
This language version has not yet been proofread.

[1] Med *europeiska företag* avses i detta sammanhang företag inom EES som överför eller kan komma att överföra personuppgifter till företag i USA som är certifierade enligt dataskyddsramen mellan EU och USA.

Antaget

Innehållsförteckning

FRÅGA 1. VAD ÄR RAMEN FÖR DATASKYDD MELLAN EU OCH USA?

Ramen för dataskydd mellan EU och USA är en självcertifieringsmekanism för företag i USA. Företag som självcertifieras enligt dataskyddsramen förbinder sig att följa de principer och regler och uppfylla de skyldigheter som gäller för behandlingen av uppgifter som tillhör privatpersoner inom EES. För mer information om dessa åtaganden, se dataskyddsramens principer.[2]

Europeiska kommissionen anser att överföringar av personuppgifter från EES till företag som certifierats enligt dataskyddsramen åtnjuter en adekvat skyddsnivå.[3] Detta innebär att personuppgifter fritt kan överföras till företag i USA som erhållit denna certifiering, utan att ytterligare skyddsåtgärder behöver vidtas eller tillstånd inhämtas. Relevanta länkar för mer information:

- Europeiska kommissionens Frågor och svar: Ramen för dataskydd mellan EU och USA[4]
- Dataskyddsramens webbplats, som förvaltas av Förenta staternas handelsministerium[5]
- Europeiska kommissionens beslut om en adekvat skyddsnivå för personuppgifter inom ramen för dataskydd mellan EU och Förenta staterna[6]

Ramen för dataskydd gäller för alla typer av personuppgifter som överförs från EES till USA, inklusive personuppgifter som behandlas för kommersiella eller hälsorelaterade ändamål och personalrelaterad information som samlas in inom ramen för anställningsförhållanden (nedan kallad *personalinformation*), så länge som det mottagande företaget i USA har erhållit självcertifiering enligt dataskyddsramen för att behandla dessa typer av uppgifter.[7]

FRÅGA 2. VILKA FÖRETAG FRÅN USA HAR RÄTT TILL SJÄLVCERTIFIERING ENLIGT RAMEN FÖR DATASKYDD MELLAN EU OCH USA?

För att vara berättigade till självcertifiering enligt dataskyddsramen måste företagen i USA vara underordnade de utrednings- och verkställighetsbefogenheter som innehas av Förenta staternas federala konkurrensmyndighet (Federal Trade Commission, FTC) eller transportministerium (Department of Transportation, DoT). Andra amerikanska lagstadgade organ kan komma att inkluderas i framtiden.[8]

---

[2] https://www.dataprivacyframework.gov/program-articles/Participation-Requirements-Data-Privacy-Framework-(DPF)-Principles

[3] Beslutet om en ram för dataskydd med en adekvat skyddsnivå antogs av Europeiska kommissionen den 10 juli 2023. Ramen har utformats gemensamt av Europeiska kommissionen och Förenta staternas handelsministerium och ersätter genomförandebeslut (EU) 2016/1250 om skölden för skydd av privatlivet, som ogiltigförklarades av EU-domstolen den
16 juli 2020 genom mål C-311/18, *Data Protection Commissioner mot Facebook Ireland Limited och Maximillian Schrems (Schrems II)*.

[4] https://ec.europa.eu/commission/presscorner/detail/en/qanda_23_3752

[5] https://www.dataprivacyframework.gov/s/

[6] https://commission.europa.eu/system/files/2023-07/Adequacy%20decision%20EU-US%20Data%20Privacy%20Framework_en.pdf

[7] Observera att vissa självcertifieringar enligt dataskyddsramen inte omfattar personalinformation. I tillämpliga fall är det därför viktigt att kontrollera om så är fallet. Se även Fråga 3.

[8] Se punkt I.2 i bilaga I till beslutet om adekvat skyddsnivå, om principerna för ramen om dataskydd mellan EU och USA, utfärdat av Förenta staternas handelsministerium.

Detta innebär att exempelvis ideella organisationer, banker, försäkringsbolag och leverantörer av telekommunikationstjänster (i samband med gemensam transportverksamhet) som faller utanför transportministeriets eller konkurrensmyndighetens jurisdiktion inte kan självcertifiera sig enligt dataskyddsramen.

FRÅGA 3. VAD SKA JAG GÖRA INNAN JAG ÖVERFÖR PERSONUPPGIFTER TILL ETT FÖRETAG I USA SOM ÄR ELLER PÅSTÅR SIG VARA CERTIFIERAT ENLIGT RAMEN FÖR DATASKYDD MELLAN EU OCH USA?

Innan en uppgiftsutförare inom EES överför personuppgifter till ett företag i USA som påstår sig vara självcertifierat enligt dataskyddsramen måste denna uppgiftsutförare försäkra sig om att företaget i USA har en gällande självcertifiering (certifieringar måste förnyas årligen) och att denna certifiering omfattar personuppgiftstypen i fråga (särskilt huruvida certifieringen avser personalinformation eller icke-personalinformation).[9]

För att kontrollera om en självcertifiering gäller och är tillämplig måste uppgiftsutförarna i EES kontrollera om företaget i USA finns med i dataskyddsramens förteckning,[10] som finns tillgänglig på Förenta staternas handelsministeriums webbplats. I denna förteckning ingår även ett register över företag som har tagits bort från förteckningen (”inactive participants”, dvs. inaktiva deltagare). För vart och ett av dessa företag anges också orsaken till att de tagits bort. Överföringar av personuppgifter till sådana företag från uppgiftsutförare i EES omfattas inte av dataskyddsramen. Observera att företag som har strukits från dataskyddsramens förteckning måste fortsätta att tillämpa dataskyddsramens principer på personuppgifter som mottagits under den tid som de varit certifierade enligt dataskyddsramen, så länge de lagrar dessa uppgifter.

För överföring av personuppgifter till företag i USA som inte (eller inte längre) är självcertifierade enligt dataskyddsramen kan andra grunder för överföring användas enligt vad som anges i kapitel V i den allmänna dataskyddsförordningen, exempelvis bindande företagsbestämmelser eller standardavtalsklausuler.

Genom att uppgiftsmottagaren i USA är självcertifierad enligt dataskyddsramen kan uppgiftsexportörer i EES uppfylla kraven i kapitel V i den allmänna dataskyddsförordningen. Alla övriga krav i den allmänna dataskyddsförordningen och i gällande nationell dataskyddslagstiftning fortsätter också att gälla.

3.1. Överföringar till amerikanska dotterbolag till företag som certifierats enligt ramen för dataskydd mellan EU och USA

När det gäller överföringar till företag i USA som är dotterföretag till moderbolag som är certifierade enligt dataskyddsramen, måste uppgiftsutförare i EES kontrollera om moderbolagets certifiering även omfattar dotterbolaget i fråga.

[9] Se definitionen av personalinformation under Fråga 1.
[10] https://www.dataprivacyframework.gov/list

Ytterligare information om hur man kontrollerar omfattningen av en organisations självcertifiering, inklusive om andra enheter eller dotterbolag i USA omfattas av den, finns här.[11]

3.2. Överföring till ett företag i USA som fungerar som personuppgiftsansvarig

Innan personuppgifter överförs till en personuppgiftsansvarig i USA måste en uppgiftsutförare inom EES säkerställa att överföringen uppfyller alla relevanta bestämmelser i den allmänna dataskyddsförordningen. Som ett första steg kan uppgiftsutföraren endast dela personuppgifter med ett företag i USA om det finns en rättslig grund för behandlingen (artikel 6 i den allmänna dataskyddsförordningen). Dessutom måste alla andra krav i den allmänna dataskyddsförordningen uppfyllas (t.ex. ändamålsbegränsning, proportionalitet, korrekthet och informationsskyldigheter gentemot de registrerade). Observera att när uppgifter ska överföras till ett självcertifierat företag i USA måste uppgiftsutföraren i EES, i enlighet med artiklarna 13 och 14 i den allmänna dataskyddsförordningen, informera de registrerade om identiteten på mottagarna av deras uppgifter och om att överföringen omfattas av beslutet om en dataskyddsram med adekvat skyddsnivå mellan EU och USA.

3.3. Överföring till ett företag i USA som agerar som personuppgiftsbiträde

När en personuppgiftsansvarig i EES överför uppgifter till ett personuppgiftsbiträde i USA är den personuppgiftsansvarige och personuppgiftsbiträdet skyldiga att ingå ett avtal om behandling av personuppgifter enligt artikel 28 i den allmänna dataskyddsförordningen (nedan kallat *databehandlingsavtal*), oavsett om personuppgiftsbiträdet är självcertifierat enligt dataskyddsramen.

Du hittar mer information om villkoren för detabehandlingsavtal för överföringar till ett personuppgiftsbiträde i USA här.[12]

Ingående av ett databehandlingsavtal krävs för att säkerställa att personuppgiftsbiträdet från USA åtar sig att

- endast behandla personuppgifter på dokumenterade instruktioner från den personuppgiftsansvarige, inbegripet när det gäller överföringar av personuppgifter till ett tredjeland eller en internationell organisation, såvida inte denna behandling krävs enligt unionsrätten eller enligt en medlemsstats nationella rätt som personuppgiftsbiträdet omfattas av, och i så fall informera den personuppgiftsansvarige om det rättsliga kravet innan uppgifterna behandlas, såvida sådan information inte är förbjuden med hänvisning till ett viktigt allmänintresse enligt denna rätt,
- säkerställa att personer som har tillstånd att behandla personuppgifterna har åtagit sig att iaktta sekretess eller omfattas av en lämplig lagstadgad tystnadsplikt,
- genomföra lämpliga tekniska och organisatoriska åtgärder för att säkerställa en säkerhetsnivå som är lämplig i förhållande till risken, i linje med vad som krävs i databehandlingsavtalet (som härrör från artikel 32 i den allmänna dataskyddsförordningen) och avsnitten 4 och 10 i dataskyddsramen mellan EU och USA,

[11] https://www.dataprivacyframework.gov/program-articles/How-to-Verify-an-Organization-s-Privacy-Data-Privacy-Framework-(DPF)-Commitments

[12] https://www.dataprivacyframework.gov/program-articles/Contract-Requirements-for-Data-Transfers-to-a-Processor

- respektera de villkor som anges i databehandlingsavtalet (som härrör från artikel 28.2 och 28.4 i den allmänna dataskyddsförordningen) och avsnitt II.3.B i dataskyddsförordningen för att anlita ett annat personuppgiftsbiträde,
- med tanke på behandlingens art, hjälpa den personuppgiftsansvarige genom lämpliga tekniska och organisatoriska åtgärder, i den mån detta är möjligt, så att den personuppgiftsansvarige kan fullgöra sin skyldighet att svara på begäran om utövande av den registrerades rättigheter i enlighet med kapitel III i den allmänna dataskyddsförordningen,
- bistå den personuppgiftsansvarige med att se till att skyldigheterna enligt artiklarna 32–36 fullgörs, med beaktande av typen av behandling och den information som personuppgiftsbiträdet har att tillgå,
- beroende på vad den personuppgiftsansvarige väljer, radera eller återlämna alla personuppgifter till den personuppgiftsansvarige efter det att tillhandahållandet av behandlingstjänster har avslutats samt radera befintliga kopior, såvida inte lagring av personuppgifterna krävs enligt unionsrätten eller medlemsstaternas nationella rätt,
- ge den personuppgiftsansvarige tillgång till all information som krävs för att påvisa fullgörandet av de skyldigheter som fastställs i artikel 28 i den allmänna dataskyddsförordningen samt möjliggöra och bidra till granskningar, inbegripet inspektioner, som genomförs av den personuppgiftsansvarige eller av en annan revisor som bemyndigats av den personuppgiftsansvarige. När det gäller den sista punkten ska personuppgiftsbiträdet omedelbart underrätta den personuppgiftsansvarige om det anser att en instruktion strider mot dataskyddsramen mellan EU och USA.

Om personuppgiftsbiträdet i USA anlitar ett annat personuppgiftsbiträde för att utföra specifik behandling på uppdrag av den personuppgiftsansvarige i EES, måste personuppgiftsbiträdet säkerställa att kraven i avsnitt II.3.B i dataskyddsramen är uppfyllda. Detta inbegriper att säkerställa att det andra personuppgiftsbiträdet tillhandahåller samma skyddsnivå för personuppgifterna som den som krävs enligt dataskyddsramen mellan EU och USA, och uppfyller samma dataskyddsskyldigheter som de som anges i databehandlingsavtalet. Om det andra personuppgiftsbiträdet inte fullgör sina skyldigheter i fråga om dataskydd ska det ursprungliga personuppgiftsbiträdet vara fullt ansvarigt gentemot den personuppgiftsansvarige för utförandet av det andra personuppgiftsbiträdets skyldigheter.

FRÅGA 4. VAR KAN JAG FÅ VÄGLEDNING OM CERTIFIERING AV AMERIKANSKA DOTTERBOLAG TILL EUROPEISKA FÖRETAG?

Amerikanska dotterbolag till företag inom EES kan självcertifiera sig enligt dataskyddsramen mellan EU och USA om de är underordnade de behörigheter som USA:s federala konkurrensmyndighet (Federal Trade Commission, FTC) eller transportministerium (Department of Transportation, DoT) innehar.

Du hittar mer information om behörighetskraven här,[13] och en guide till självcertifieringsprocessen här.[14]

[13] https://www.dataprivacyframework.gov/program-articles/U-S-Subsidiaries-of-European-Businesses-Participation-in-the-Data-Privacy-Framework-(DPF)-Program

[14] https://www.dataprivacyframework.gov/program-articles/How-to-Join-the-Data-Privacy-Framework-(DPF)-Program-(part%E2%80%931)