

EU-USA-DATABESKYTTELSESRAMMEN

FAQ FOR EUROPÆISKE VIRKSOMHEDER¹

Vedtaget den 16. juli 2024

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

¹ I denne sammenhæng henviser europæiske virksomheder til virksomheder i EØS, der overfører eller kan overføre personoplysninger til virksomheder i USA, der er certificeret i henhold til databeskyttelsesrammen.

Indholdsfortegnelse

Spørgsmål 1. Hvad er EU-USA-databeskyttelsesrammen?.....	3
Spørgsmål 2. Hvilke amerikanske virksomheder kan deltage i EU-USA-databeskyttelsesrammen?.....	3
Spørgsmål 3. Hvad skal jeg gøre, før jeg overfører personoplysninger til en virksomhed i USA, som er eller hævder at være certificeret i henhold til EU-USA-databeskyttelsesrammen?.....	4
Spørgsmål 4. Hvor finder jeg vejledning vedrørende certificering af amerikanske datterselskaber af europæiske virksomheder?	6

SPØRGSMÅL 1. HVAD ER EU-USA-DATABESKYTTELSESRAMMEN?

EU-USA-databeskyttelsesrammen er en selvcertificeringsmekanisme for virksomheder i USA. Virksomheder, der er selvcertificeret i henhold til databeskyttelsesrammen, skal overholde databeskyttelsesrammens principper, regler og forpligtelser i forbindelse med behandlingen af personoplysninger, der tilhører enkeltpersoner i EØS. For mere information om disse forpligtelser, se [databeskyttelsesrammens principper](#).²

Europa-Kommissionen fandt, at overførsler af personoplysninger fra EØS til virksomheder i USA, der er certificeret i henhold til databeskyttelsesrammen, nyder et tilstrækkeligt beskyttelsesniveau.³ Som følge heraf kan personoplysninger overføres frit til certificerede virksomheder i USA, uden at det er nødvendigt at indføre yderligere garantier eller indhente en godkendelse. Her er nogle relevante links til mere information:

- Europa-Kommissionens [Spørgsmål og svar: databeskyttelsesrammen](#)⁴
- [Databeskyttelsesrammewebstedet, der administreres af det amerikanske handelsministerium](#)⁵
- [Europa-Kommissionens afgørelse om et tilstrækkeligt beskyttelsesniveau for personoplysninger i henhold til EU-USA-databeskyttelsesrammen](#)⁶

Databeskyttelsesrammen omfatter alle typer af personoplysninger, der overføres fra EØS til USA, herunder personoplysninger, der behandles til kommercielle eller sundhedsmæssige formål, og oplysninger relateret til menneskelige ressourcer, der indsamles i forbindelse med et ansættelsesforhold (i det følgende benævnt: "HR-oplysninger"), så længe den modtagende virksomhed i USA er selvcertificeret i henhold til databeskyttelsesrammen til at behandle disse typer af oplysninger.⁷

SPØRGSMÅL 2. HVILKE AMERIKANSKE VIRKSOMHEDER KAN DELTAGE I EU-USA-DATABESKYTTELSESRAMMEN?

For at være berettiget til at foretage selvcertificering i henhold til databeskyttelsesrammen skal en virksomhed i USA være underlagt undersøgelses- og håndhævelsesbeføjelser ved den amerikanske

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

³ Afgørelsen om tilstrækkeligheden af databeskyttelsesrammen blev vedtaget af Europa-Kommissionen den 10. juli 2023. Den blev udformet af Europa-Kommissionen og det amerikanske handelsministerium og erstatter afgørelsen om EU's og USA's værn om privatlivets fred (afgørelse (EU) 2016/1250), som blev erklæret ugyldig af EU-Domstolen

den 16. juli 2020 i sag C-311/18, *Data Protection Commissioner mod Facebook Ireland Limited and 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 Bemærk, at ikke alle selvcertificeringer under databeskyttelsesrammen omfatter HR-oplysninger. Det er derfor vigtigt at undersøge, om dette er tilfældet, hvis det er relevant. Se også spørgsmål 3.

Federal Trade Commission eller det amerikanske transportministerium. Andre amerikanske lovbestemte organer kan inddrages i fremtiden.⁸

Det betyder f.eks., at nonprofitorganisationer, banker, forsikringsselskaber og telekommunikationsudbydere (af fælles bærertjenester), som ikke er underlagt beføjelser ved Federal Trade Commission eller det amerikanske transportministerium, ikke kan foretage selvcertificering i henhold til databeskyttelsesrammen.

SPØRGSMÅL 3. HVAD SKAL JEG GØRE, FØR JEG OVERFØRER PERSONOPLYSNINGER TIL EN VIRKSOMHED I USA, SOM ER ELLER HÆVDER AT VÆRE CERTIFICERET I HENHOLD TIL EU-USA- DATABESKYTTELSESRAMMEN?

Inden en dataeksportør i EØS overfører personoplysninger til en virksomhed i USA, som hævder at have foretaget selvcertificering i henhold til databeskyttelsesrammen, skal vedkommende sikre sig, at virksomheden i USA har en aktiv selvcertificering (certificeringer skal fornyes årligt), og at denne certificering omfatter de pågældende oplysninger (navnlig om den omfatter HR-oplysninger/ikke-HR-oplysninger).⁹

For at verificere, om en selvcertificering er aktiv og gældende, skal dataeksportører i EØS kontrollere, om virksomheden i USA er opført på [listen over deltagere i databeskyttelsesrammen](#)¹⁰ på det amerikanske handelsministeriums websted. Denne liste omfatter også et register over virksomheder, der er blevet fjernet fra listen ("inaktive deltagere"), med angivelse af årsagerne til deres fjernelse. Dataeksportører i EØS kan ikke påkalde sig databeskyttelsesrammen, når de overfører personoplysninger til sådanne virksomheder. Bemærk, at virksomheder, der er blevet fjernet fra listen over deltagere i databeskyttelsesrammen, fortsat skal anvende databeskyttelsesrammens principper på personoplysninger, de modtog, mens de deltog i databeskyttelsesrammen, så længe de opbevarer disse oplysninger.

I forbindelse med overførsel af personoplysninger til virksomheder i USA, der ikke (eller ikke længere) er selvcertificerede i henhold til databeskyttelsesrammen, kan andre grunde til overførsel i henhold til kapitel V i GDPR anvendes, f.eks. bindende virksomhedsregler eller standardkontraktbestemmelser.

Det forhold, at modtageren i USA er selvcertificeret i henhold til databeskyttelsesrammen, vil gøre det muligt for dataeksportører i EØS at overholde kapitel V i GDPR, men alle andre krav i GDPR og enhver anden national databeskyttelseslovgivning finder fortsat anvendelse.

3.1. Overførsler til amerikanske datterselskaber af virksomheder, der er certificeret i henhold til EU-USA-databeskyttelsesrammen

⁸ Se bilag I til afgørelsen om tilstrækkeligheden af beskyttelsesniveauet, EU-USA-databeskyttelsesrammens principper udstedt af det amerikanske handelsministerium, afsnit I.2.

⁹ Se definitionen af HR-oplysninger i spørgsmål 1.

¹⁰ <https://www.dataprivacyframework.gov/list>

I tilfælde af overførsler til virksomheder i USA, der er datterselskaber af et moderselskab, der er certificeret i henhold til databeskyttelsesrammen, skal dataeksportører i EØS kontrollere, om moderselskabets certificering også dækker det pågældende datterselskab.

Du kan finde yderligere information om, hvordan du verificerer omfanget af en organisations selvcertificering, herunder om andre amerikanske enheder eller amerikanske datterselskaber er omfattet heraf, [her](#).¹¹

3.2. Overførsler til en virksomhed i USA, der fungerer som dataansvarlig

Inden personoplysninger overføres til en dataansvarlig i USA, skal en dataeksportør i EØS sikre, at overførslen er i overensstemmelse med alle relevante bestemmelser i GDPR. Som et første skridt kan dataeksportøren kun dele personoplysninger med en virksomhed i USA, hvis der er et retsgrundlag for behandlingen (artikel 6 i GDPR). Desuden skal alle andre krav i GDPR opfyldes (f.eks. med hensyn til formålsbegrænsning, proportionalitet, rigtighed og oplysningspligt over for registrerede). Bemærk, at når oplysninger skal overføres til en selvcertificeret virksomhed i USA, skal dataeksportøren i EØS i henhold til artikel 13 og 14 i GDPR informere de registrerede om identiteten på modtagerne af deres oplysninger og om, at overførslen er omfattet af afgørelsen om tilstrækkeligheden af EU-USA-databeskyttelsesrammen.

3.3. Overførsler til en virksomhed i USA, der fungerer som databehandler

Når en dataansvarlig i EØS overfører oplysninger til en databehandler i USA, er den dataansvarlige og databehandleren forpligtet til at indgå en aftale om databehandling i henhold til artikel 28 i GDPR (i det følgende benævnt: databehandlingsaftale), uanset om databehandleren er selvcertificeret i henhold til databeskyttelsesrammen.

Du kan finde mere information om kontraktkravene i forbindelse med overførsler til en databehandler i USA [her](#).¹²

Indgåelse af en databehandlingsaftale er nødvendig for at sikre, at den amerikanske databehandler forpligter sig til:

- kun at behandle personoplysninger efter dokumenteret instruks fra den dataansvarlige, herunder for så vidt angår videregivelse af personoplysninger til et tredjeland eller en international organisation, medmindre det kræves i henhold til EU-ret eller medlemsstatsret, som databehandleren er underlagt; i så fald underretter databehandleren den dataansvarlige om dette retlige krav inden behandlingen, medmindre den pågældende ret forbyder en sådan underretning af hensyn til vigtige samfundsmæssige interesser
- at sikre, at personer med bemyndigelse til at behandle personoplysningerne har forpligtet sig til at overholde en tavshedspligt eller er underlagt en passende vedtægtsmæssig tavshedspligt
- at gennemføre behørigte tekniske og organisatoriske foranstaltninger for at sikre et sikkerhedsniveau, der er passende i forhold til risikoen, i overensstemmelse med, hvad

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

der kræves i henhold til databehandlingsaftalen (jf. artikel 32 i GDPR) og afsnit 4 og 10 i databeskyttelsesrammen

- at overholde de betingelser, der er omhandlet i databehandlingsaftalen (jf. artikel 28, stk. 2 og 4, i GDPR) og afsnit II.3.B i databeskyttelsesrammen, for ansættelse af en anden databehandler
- under hensyntagen til behandlingens karakter, så vidt muligt at bistå den dataansvarlige ved hjælp af passende tekniske og organisatoriske foranstaltninger med opfyldelse af den dataansvarliges forpligtelse til at besvare anmodninger om udøvelse af de registreredes rettigheder som fastlagt i kapitel III i GDPR
- at bistå den dataansvarlige med at sikre overholdelse af forpligtelserne i medfør af artikel 32-36 i GDPR under hensyntagen til behandlingens karakter og den information, der er tilgængelig for databehandleren
- efter den dataansvarliges valg at slette eller tilbagelevere alle personoplysninger til den dataansvarlige, efter at tjenesterne vedrørende behandling er ophørt, og at slette eksisterende kopier, medmindre EU-retten eller medlemsstaternes nationale ret foreskriver opbevaring af personoplysningerne
- at stille alle oplysninger, der er nødvendige for at påvise opfyldelse af kravene i artikel 28 i GDPR, til rådighed for den dataansvarlige og at give mulighed for og bidrage til revisioner, herunder inspektioner, der foretages af den dataansvarlige eller en anden revisor, som er bemyndiget af den dataansvarlige. Med hensyn til dette sidste punkt underretter databehandleren straks den dataansvarlige, hvis en instruks efter dennes opfattelse er i strid med databeskyttelsesrammen.

Hvis den amerikanske databehandler ansætter en anden databehandler ("underdatabehandler") til at udføre specifikke behandlingsaktiviteter på vegne af den dataansvarlige i EØS, skal databehandleren sikre, at kravene i afsnit II.3.B i databeskyttelsesrammen er opfyldt. Dette omfatter sikring af, at underdatabehandleren yder det samme niveau af beskyttelse af personoplysninger som krævet i databeskyttelsesrammen og de samme databeskyttelsesforpligtelser som fastsat i databehandlingsaftalen. Hvis en underdatabehandler ikke opfylder sine databeskyttelsesforpligtelser, forbliver den oprindelige amerikanske databehandler fuldt ansvarlig over for den dataansvarlige med hensyn til opfyldelsen af denne underdatabehandlers forpligtelser.

SPØRGSMÅL 4. HVOR FINDER JEG VEJLEDNING VEDRØRENDE CERTIFICERING AF AMERIKANSKE DATTERSELSKABER AF EUROPÆISKE VIRKSOMHEDER?

Amerikanske datterselskaber af EØS-virksomheder kan foretage selvcertificering i henhold til databeskyttelsesrammen, hvis de er underlagt beføjelser ved Federal Trade Commission eller det amerikanske transportministerium.

Du kan finde mere information om egnethedskravene [her](#),¹³ og en vejledning til selvcertificeringsprocessen [her](#).¹⁴

¹³[https://www.dataprivacyframework.gov/program-articles/U-S-Subsidiaries-of-European-Businesses-Participation-in-the-Data-Privacy-Framework-\(DPF\)-Program](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-\(part%E2%80%93\)](https://www.dataprivacyframework.gov/program-articles/How-to-Join-the-Data-Privacy-Framework-(DPF)-Program-(part%E2%80%93))