Datum
2023-09-25

Diarienummer
20230921:165

Dataskyddsombudets PM med rekommendationer efter adekvansbeslutet *EU-US Data Privacy Framework*

Innehåll

Sammanfattning 1
1. Vad är problemet med tredjelandsöverföringar? 2
2. Vad innebär *Ramverket*? 2
3. Upphävs tidigare regler? 3
4. Har *Ramverket* överklagats? 3
5. Vilka brister kan finns i *Ramverket*? 3
6. Dataskyddsombudet rekommenderar 6

Sammanfattning

Den 10 juli 2023 har EU-kommissionen antagit ett beslut om adekvat skydd för personuppgifter mellan EU och USA. Beslutet kallas *EU-US Data Privacy Framework* (fortsättningsvis *Ramverket*).[1] Beslutet innebär att personuppgifter får överföras från EU till amerikanska bolag utan att ytterligare skyddsåtgärder behöver sättas in, *om* det amerikanska bolaget självcertifierat sig och registrerat sig på en *deltagarlista*[2]. *Ramverket* har redan överklagats.

I denna PM redogörs för *Ramverket* och dess eventuella brister. Dataskyddsombudet lämnar slutligen sina rekommendationer till kommunen på sid 6.

[1] https://commission.europa.eu/system/files/2023-0/Adequacy%20decision%20EU-US%20Data%20Privacy%20Framework_en.pdf; läs mer här; https://ec.europa.eu/commission/presscorner/detail/sv/qanda_23_3752, https://ec.europa.eu/commission/presscorner/detail/sv/ip_23_3721, https://ec.europa.eu/commission/presscorner/detail/en/fs_23_3754, den 5 september 2023.
[2] https://www.dataprivacyframework.gov/s/participant-search.

Postadress
Danderyds kommun
Dataskyddsombud
Box 66
182 05 DJURSHOLM

Besöksadress

Växel
08-588 910 00

Direkt

E-post
dataskydd@danderyd.se

Webb
www.danderyd.se

1. Vad är problemet med tredjelandsöverföringar?

Amerikanska bolag har växt sig starka på den digitala marknaden och kan ha resurser som kommunen inte har. Dessvärre faller bolag med säte i USA under amerikansk lagstiftning som innebär att amerikanska myndigheter kan inhämta personuppgifter underhand hos amerikanska bolag.

Denna underhandsinhämtning är dock inte förenlig med (den europeiska) dataskyddsförordningen eller svenska sekretesslagstiftningen och här uppstår problematiken.

2. Vad innebär *Ramverket*?

EU-kommissionen har den 10 juli 2023 antagit *EU-US Data Privacy Framework* (fortsättningsvis *Ramverket*).[3] De stora penseldragen i *Ramverket* är följande.

- *Ramverket* innebär att personuppgifter får överföras från EU till amerikanska bolag utan att ytterligare skyddsåtgärder behöver sättas in, *om* bolagen registrerat sig på en *deltagarlista*[4] som hanteras av amerikanska myndigheter.
- EU-kommissionen har bedömt att USA upprätthåller *en adekvat skyddsnivå* för personuppgifterna.
- *Ramverket* utgår ifrån en amerikansk antagen *presidentorder 14086*[5] med följande förordningar, som innebär följande.
    - De amerikanska underrättelsemyndigheternas tillgång till personuppgifter från EU begränsas till vad som är *nödvändigt* och *proportionerligt* för att skydda den *nationella säkerheten*.
    - Tillsynen av den amerikanska underrättelseverksamheten utökas.
    - En oberoende amerikansk dataskyddsdomstol[6], *Data Protection Review Court*, inrättas.[7]

---

[3] https://commission.europa.eu/system/files/2023-0/Adequacy%20decision%20EU-US%20Data%20Privacy%20Framework_en.pdf; läs mer här; https://ec.europa.eu/commission/presscorner/detail/sv/qanda_23_3752, https://ec.europa.eu/commission/presscorner/detail/sv/ip_23_3721, https://ec.europa.eu/commission/presscorner/detail/en/fs_23_3754, den 5 september 2023.
[4] https://www.dataprivacyframework.gov/s/participant-search.
[5] https://www.govinfo.gov/content/pkg/FR-2022-10-14/pdf/2022-22531.pdf
[6] https://www.justice.gov/opcl/redress-data-protection-review-court
[7] Förfarandet går till så att den enskilde lämnar klagomål till nationell dataskyddsmyndighet (jfr. Integritetsskyddsmyndigheten). Därefter lämnas klagomålet vidare till den amerikanska underrättelsetjänstens ombudsman, *Civil Liberties Protection Officer*, som

- De amerikanska bolagen certifierar sig själva för att registrera sig på *deltagarlistan*[8], vilket ska visa på att bolagen åtagit sig vissa skyldigheter; som till exempel ändamålsbegränsning, uppgiftsminimering och gallring av uppgifter som inte längre behövs.
- Uppföljning ska ske inom ett år från ikraftträdandet.

Ramverket ersätter *Safe Harbour* och *Privacy Shield* som tidigare har upphävts av EU-domstolen.

3. Upphävs tidigare regler?

- Nej, *Ramverket* upphäver inte dataskyddsförordningen[9] utan den och kraven där i fortsätter att gälla. Det innebär att rättslig grund för behandlingen måste finnas och principerna och personers fri- och rättigheter ska följas med mera.
- *Ramverket* innebär inte att det är fritt fram att överföra sekretessbelagda uppgifter till amerikanska bolag, utan offentlighets- och sekretesslagen (2009:400) gäller fortfarande.

4. Har *Ramverket* överklagats?

- Ja, en parlamentsledamot har, i egenskap av privatperson, överklagat *Ramverket*.
- Organisationen *None of your business* (fortsättningsvis NOYB) har deklarerat att de kommer överklaga *Ramverket*.[10]

5. Vilka brister kan finns i *Ramverket*?

Den stora frågan är alltså om EU-kommissionen gjort en korrekt bedömning om den adekvata skyddsnivån i USA.[11]

- ”*We would need changes in US surveillance law to make this work - and we simply don't have it.*”, Max Schrems, NOYB:s grundare om *Ramverket*.[12]

---

avkunnar ett beslut. Beslutet kan överklagas till den nyinrättade dataskyddsdomstolen. Finner dataskyddsdomstolen att personuppgifterna har inhämtats i strid med *presidentordern*, kan domstolen beordra att personuppgifterna raderas.

[8] https://www.dataprivacyframework.gov/s/participant-search.

[9] https://eur-lex.europa.eu/legal-content/SV/TXT/PDF/?uri=CELEX:32016R0679

[10] https://noyb.eu/en/european-commission-gives-eu-us-data-transfers-third-round-cjeu, den 6 september 2023.

[11] Art 45.2 dataskyddsförordningen, https://eur-lex.europa.eu/legal-content/SV/TXT/PDF/?uri=CELEX:32016R0679.

- Europeiska dataskyddsstyrelsen[13] (*European Data Protection Board, EDPB)*, har identifierat flera brister i *Ramverket* till exempel i förhållande till den registrerades rättigheter, avsaknad av förhandstillstånd för massinsamling (”bulk”), gallring, spridning och rättsmedel i praktiken. Vidare finns vissa redan identifierade brister i upphävda *Privacy Shield,* kvar i *Ramverke*t.[14]

Utöver nämnda påtalade brister ovan, kan även identifieras andra brister i *Ramverket*.

- Inom Sverige och EU tillförsäkras enskilda en mängd rättigheter som respekt för privat- och familjeliv (kommunikation)[15], skydd av personuppgifter[16], rätt till effektivt rättsmedel[17], rätt till privatliv och rättvis rättegång[18] samt att enskilda har ett skydd mot betydande intrång i den personliga integriteten.[19] Därutöver finns även dataskyddsförordningsspecifika rättigheter som rätt till radering, rättelse, information med flera som också måste tillgodoses.[20]

  Emellertid har inte EU-medborgare inte motsvarande rättigheter i USA. EU-medborgare har till exempel inte något lagstadgat skydd mot obefogad husrannsakan och konfiskation.[21] Hur ska enskilda tillförsäkras sina EU-rättigheter när uppgifterna förs över till USA?

---

[12] https://noyb.eu/en/european-commission-gives-eu-us-data-transfers-third-round-cjeu, den 6 september 2023.
[13] Art 68-70 dataskyddsförordningen, https://eur-lex.europa.eu/legal-content/SV/TXT/PDF/?uri=CELEX:32016R0679.
[14] https://edpb.europa.eu/system/files/2023-02/edpb_opinion52023_eu-us_dpf_en.pdf, https://www.imy.se/nyheter/edpb-yttrar-sig-om-eu-us-data-privacy-framework/.
[15] Art 7, 8 och 47 Europeiska unionens stadga om de grundläggande rättigheterna, https://eur-lex.europa.eu/legal-content/SV/TXT/?uri=CELEX:12012P/TXT
[16] Art 7, 8 och 47 Europeiska unionens stadga om de grundläggande rättigheterna, https://eur-lex.europa.eu/legal-content/SV/TXT/?uri=CELEX:12012P/TXT
[17] Art 7, 8 och 47 Europeiska unionens stadga om de grundläggande rättigheterna, https://eur-lex.europa.eu/legal-content/SV/TXT/?uri=CELEX:12012P/TXT
[18] Art 6, 8 och 12 Lag (1994:1219) om den europeiska konventionen angående skydd för de mänskliga rättigheterna och de grundläggande friheterna
[19] 2 kap. 6 § regeringsformen
[20] Läs mer i kapitel 3, dataskyddsförordningen https://eur-lex.europa.eu/legal-content/SV/TXT/PDF/?uri=CELEX:32016R0679.
[21] Jfr. till exemepel 4th Amendment: *”The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.”,*
https://constitution.congress.gov/constitution/amendment-4/, den 6 september 2023.

- Enligt dataskyddsförordningen ska personuppgifter hanteras konfidentiellt och säkert.[22] Är hanteringen konfidentiell och säker om åtgärder vidtas med personuppgifterna som kommunen inte styr över eller kan kontrollera, av främmande makt?
- De personuppgiftsansvariga nämnderna har ett personuppgiftsansvar enligt dataskyddsförordningen. Hur upprätthålls personuppgiftsansvaret om åtgärder vidtas med personuppgifterna som nämnden inte styr över eller kan kontrollera?
- Enligt offentlighets- och sekretesslagen (2009:400) får sekretessbelagda uppgifter inte röjas.[23] Hur upprätthålls sekretessen om åtgärder vidtas med personuppgifterna utan att sekretessbedömning skett?
- Ramverket baseras på USA:s *presidentorder 14086*. En presidentorder utgör inte lagstiftning och kan upphävas. Grunden för *Ramverket* är alltså ganska skör. Det kan även finnas andra amerikanska styrande dokument för underrättelseinhämtning med annat innehåll, som inte är kända.
- Även om amerikansk underrättelseverksamhet måste vara *nödvändig* och *proportionell*, finns ingen definition vad det egentligen innebär och var gränsen går.
- En olaglig behandling av personuppgifter kan inte läkas genom inrättandet av en amerikansk dataskyddsdomstol.
- De bolag som har registrerat sig på den tidigare deltagarlistan för *Privacy Shield*, behöver inte registrera sig på nytt på *deltagarlistan*[24] för *Ramverket*, vilket visar på att bolagen rent faktiskt inte behövt vidta några ytterligare åtgärder än tidigare under *Privacy Shield*, trots att EU-domstolen redan har underkänt de åtgärderna.

Sammantaget har några närmande steg tagits mellan USA och EU genom *Ramverket*, men det är inte självklart att *Ramverket* är tillräckligt för att anses uppnå full GDPR-efterlevnad. Ramverket kommer prövas rättsligt i och med att det har överklagats.

---

[22] Art 5 dataskyddsförordningen, https://eur-lex.europa.eu/legal-content/SV/TXT/PDF/?uri=CELEX:32016R0679.
[23] Jfr. 2 kap. 1 § offentlighets- och sekretesslagen (2009:400).
[24] https://www.dataprivacyframework.gov/s/participant-search.

6. Dataskyddsombudet rekommenderar

Kommunen ska vara medveten om att adekvansbeslutet kommer att prövas rättsligt, och att det kan komma att upphävas. Utifrån denna hypotes rekommenderas att kommunen gör följande.

- Skriv eventuella avtal med amerikanska leverantörer med avtalsklausul om att avtalet kan sägas upp med kort varsel och utan att vite ska utgå, för det fall *Ramverket* upphävs eller om leverantören/underleverantören inte längre är certifierad på *deltagarlistan*[25].
    - Fundera rent praktiskt på hur verksamheten ska hantera om *Ramverket* upphävs eller leverantör/underleverantörer inte längre är certifierad på *deltagarlistan*[26]. Finns plan B? Går det att plocka hem personuppgifterna?
- Fortsätta identifiera, dokumentera och vara vaksam vid alla typer en tredjelandsöverföring av personuppgifter utanför EU/EES. Identifiera de aktuella personuppgifterna det gäller och fortsätt att göra konsekvensbedömningar[27].
    - Rör det *känsliga personuppgifter,*[28] *extra skyddsvärda personuppgifter*[29] samt *sekretessbelagda uppgifter* måste både lagligheten och lämpligheten begrundas.
    - Beakta den registrerades fri- och rättigheter. Respekteras enskilds rätt till privatliv och skydd för personuppgifter? Tillhandahålls de dataskyddsförordningsspecifika rättigheterna som radering, rättelse, information med flera?
    - Överväg och sätt in *riskminimerande åtgärder*. Uppgiftsminimering? Gallringsrutiner? On prem-lösningar? Pseudonymisering? Framtagande av regler och instruktioner? Avtala om hur personuppgifterna ska hanteras vid avtalets upphörande?
    - Behöver redan gjorda konsekvensbedömningar uppdateras?

---

[25] https://www.dataprivacyframework.gov/s/participant-search.
[26] https://www.dataprivacyframework.gov/s/participant-search.
[27] Art 35 dataskyddsförordningen, https://eur-lex.europa.eu/legal-content/SV/TXT/PDF/?uri=CELEX:32016R0679.
[28] Som hälsa, facklig tillhörighet, etnisk bakgrund, religion med flera, se art 9, dataskyddsförordningen, https://eur-lex.europa.eu/legal-content/SV/TXT/PDF/?uri=CELEX:32016R0679.
[29] Som uppgifter om barn, personnummer, integritetskänsliga uppgifter.

- Säkerställ att aktuell verksamhetsgren för det tilltänkta amerikanska bolaget anges på *deltagarlistan*.[30]
- Fundera på lämpligheten. *Vad* är omdömesgillt att hantera i tredjeland?
- Fortsätt bevaka rättsutvecklingen, utvärdera och följ upp.

Anne Hännestrand
dataskyddsombud

[30] https://www.dataprivacyframework.gov/s/participant-search.