Regionstyrelsens förvaltning
Personalenhet

REMISSVAR
Regionstyrelsen

Datum
2024-09-16

Diarienummer
RS 2024/1397

Finansdepartementet

Remissvar slutbetänkande Kompletterande bestämmelser till EU:s reviderade förordning om elektronisk identifiering (SOU 2024:45)

Sammanfattning av Region Dalarnas synpunkter

Region Dalarna har getts möjlighet att inkomma med remissvar gällande slutbetänkande Kompletterande bestämmelse till EU:s reviderade förordning om elektronisk identifiering (SOU 2024:45) som är utsänd av Finansdepartementet.

Region Dalarna ställer sig bakom de förslag som anges i remissen och i efterföljande avsnitt redovisas några generella synpunkter från Region Dalarna.

Generella synpunkter

Region Dalarna ställer sig bakom förslagen i sin helhet men ser samtidigt ett flertal risker med datahanteringen såsom centralisering av känsliga personuppgifter, dataintrång samt otillräckliga säkerhets- och incidenthanteringsprocesser. Brister i kontrollen över hur och av vilka uppgifter delas, samt potentiella svagheter hos privata aktörer, kan leda till negativa konsekvenser för integritet och säkerhet.

För att minska riskerna med datahanteringen i den europeiska digitala identitetsplånboken, särskilt när det gäller personuppgifter, kan följande förbättringar övervägas:

1. Stärkta säkerhetsåtgärder för centraliserad datalagring
Inför regelbundna säkerhetsrevisioner och penetrationstester för att identifiera och åtgärda sårbarheter i systemet. Krav på att alla data krypteras. Både i vila och under överföring.

2. Förbättrad kontroll över delning av personuppgifter
Skapa samtyckesmekanismer där användare kan välja exakt vilka uppgifter de vill dela, hur länge och med vilka aktörer. Samtycket ska vara tydligt och lätt att dra tillbaka.

Postadress
Region Dalarna
Box 712
791 29 Falun

Besöksadress
Region Dalarna
Vasagatan 27
Falun

Kontakt
023-49 00 00
www.regiondalarna.se
232100-0180

Handläggare
Sandra Eriksson
1:a linjens chef / Samordnare
+46720831295
sandra.a.eriksson@regiondalarna.se

3. Strängare krav och övervakning av privata tillhandahållare
Inför ett strikt certifieringssystem för privata aktörer som innefattar mer detaljerade säkerhetskrav samt krav på oberoende säkerhetsgranskningar.

4. Utökade skyddsåtgärder för GDPR-efterlevnad
Inför strikta regler för automatisk radering av personuppgifter när de inte längre är nödvändiga för de angivna ändamålen. Vidare ska användare ha en enkel och tydlig möjlighet att begära radering av sina uppgifter.

5. Förbättrad incidenthantering och rapportering
Inför ett standardiserat och snabbt rapporteringssystem som kräver omedelbar rapportering av alla incidenter, även misstänkta, till både myndigheter och användare.

6. Särskilda säkerhetskrav för privata aktörer
Inför obligatorisk säkerhetscertifiering för alla privata aktörer som vill tillhandahålla digitala identitetsplånböcker. Certifieringsprocessen bör omfatta kontinuerliga säkerhetskontroller och krav på att rapportera incidenter inom en mycket kort tidsram.

7. Decentraliserad lagring och säkerhetsmodeller
Utforska decentraliserade teknologier, såsom distribuerade ledger-teknologier (DLT) eller blockchain, för att säkerställa att data inte lagras på en enda plats, vilket minskar riskerna för massiva dataläckor.

8. Utbildning och medvetenhet
Genomför kontinuerliga utbildningsprogram för både användare och tjänsteleverantörer om bästa praxis för datasäkerhet och hur man undviker vanliga hot som phishing-attacker och social ingenjörskonst.