Regeringens proposition till riksdagen med förslag till lag om ändring av lagen om sekundär användning av personuppgifter inom social- och hälsovården

PROPOSITIONENS HUVUDSAKLIGA INNEHÅLL

I denna proposition föreslås det att kraven på informationssäkra driftmiljöer i lagen om sekundär användning av personuppgifter inom social- och hälsovården ändras så att kraven möjliggör utlämnande av i lagen avsedda uppgifter till andra informationssäkra driftmiljöer än sådana som är belägna i Finland. Syftet med ändringen är att möjliggöra användning av finländska registeruppgifter inom internationellt forskningssamarbete samtidigt som man säkerställer en hög nivå av informationssäkerhet och dataskydd.

Den föreslagna lagen avses träda i kraft den 1 december 2023.

Lagförslag

Lag

om ändring av lagen om sekundär användning av personuppgifter inom social- och hälsovården

I enlighet med riksdagens beslut

upphävs i lagen om sekundär användning av personuppgifter inom social- och hälsovården (552/2019) 21 § 2 mom.,

ändras 3 § 20 punkten, 23 § 1 mom., 25–28 §, 29 § 1 mom. och 30 § 1 mom. samt

fogas till 3 § en ny 21 punkt, till 30 § ett nytt 5 mom. och till 52 § ett nytt 3 mom. som följer:

3 §

Definitioner

I denna lag avses med

— —

20) bedömningsorgan för informationssäkerhet sådana företag, sammanslutningar och myndigheter som Transport- och kommunikationsverket med stöd av lagen om bedömningsorgan för informationssäkerhet (1405/2011) har godkänt att utföra bedömningar av om informationssystem överensstämmer med kraven i fråga om informationssäkerhet,

21) *certifieringsorgan* ett bedömningsorgan som ackrediterats enligt enhetliga internationella och europeiska bedömningsgrunder och som godkänts av ett nationellt ackrediteringsorgan enligt Europaparlamentets och rådets förordning (EG) nr 765/2008 om krav för ackreditering och marknadskontroll i samband med saluföring av produkter och upphävande av förordning (EEG) nr 339/93.

23 §

Skydd för informationssäkra driftmiljöer

En informationssäker driftmiljö ska skyddas i enlighet med statliga myndigheters skyldigheter i fråga om informationssäkerhet enligt vad som föreskrivs i 4 kap. i lagen om informationshantering inom den offentliga förvaltningen (906/2019) och vad som förutsätts i Tillståndsmyndighetens föreskrift.

— —

25 §

Påvisande av informationssäkerhet i en informationssäker driftmiljö

Informationssäkerheten i driftmiljön ska påvisas genom ett i 26 § avsett intyg från ett bedömningsorgan för informationssäkerhet eller ett certifieringsorgan.

Tillståndsmyndigheten får meddela närmare föreskrifter om de förfaranden som ska iakttas vid påvisande av informationssäkerhet samt om de certifieringsorgan som kan bedöma om driftmiljön uppfyller kraven på informationssäkerhet.

26 §

Bedömning av informationssäkerhet

Ett bedömningsorgan för informationssäkerhet bedömer i enlighet med denna lag och lagen om bedömningsorgan för informationssäkerhet, på ansökan av tjänsteleverantören, om driftmiljön uppfyller kraven på informationssäkerhet. Ett certifieringsorgan bedömer i enlighet med denna lag, på ansökan av tjänsteleverantören, om driftmiljön uppfyller kraven på informationssäkerhet. Som bedömningskriterier ska användas föreskrifter om kraven på en säker driftmiljö från Tillståndsmyndigheten.

Om driftmiljön uppfyller informationssäkerhetskraven enligt denna lag, ska bedömningsorganet för informationssäkerhet eller certifieringsorganet ge tjänsteleverantören ett intyg över sin bedömning och en anknytande kontrollrapport. Om bedömningen eller en förnyad bedömning gäller endast en del av driftmiljön, ska det i bedömningsorganets eller certifieringsorganets intyg tydligt antecknas vilken del av driftmiljön som har bedömts.

Bedömningsorganets eller certifieringsorganets intyg är i kraft högst tre år. Bedömningsorganet för informationssäkerhet eller certifieringsorganet kan av tjänsteleverantören kräva alla de uppgifter som förutsätts för bedömningen och för uppgörandet och upprätthållandet av intyget. På bedömningsorgans utfärdande av intyg tillämpas i övrigt 9 § 3 mom. i lagen om bedömningsorgan för informationssäkerhet.

27 §

Återkallande av bedömningsorganets och certifieringsorganets intyg

Om ett bedömningsorgan för informationssäkerhet eller ett certifieringsorgan konstaterar att en driftmiljö inte har uppfyllt eller inte längre uppfyller kraven i denna lag eller att ett intyg av någon annan orsak inte borde ha beviljats, ska organet uppmana tjänsteleverantören att avhjälpa bristerna. Bedömningsorganet eller certifieringsorganet får återkalla intyget för viss tid eller helt och hållet eller bevilja intyget med begränsningar, om inte tjänsteleverantören avhjälper bristerna inom den tid som organet satt ut. När tidsfristens längd bestäms ska det beaktas att en skälig tid behövs för att korrigera driftmiljön.

28 §

Anmälningsskyldighet för bedömningsorgan för informationssäkerhet och certifieringsorgan

Bedömningsorgan för informationssäkerhet och certifieringsorgan ska underrätta Tillstånds- och tillsynsverket för social- och hälsovården om alla intyg som har utfärdats, ändrats eller kompletterats eller som har återkallats för viss tid eller helt och hållet eller förvägrats och om de kontrollrapporter som avses i 26 § samt om de uppmaningar och begränsningar som avses i 27 §. Dessutom ska bedömningsorgan för informationssäkerhet och certifieringsorgan på begäran ge Tillstånds- och tillsynsverket för social- och hälsovården all behövlig ytterligare information i ärendet.

29 §

Uppföljning efter ibruktagande av informationssäker driftmiljö

Tjänsteleverantören ska genom ett uppdaterat och systematiskt förfarande följa upp och utvärdera erfarenheterna av en informationssäker driftmiljö under den tid den används för produktion. Tjänsteleverantören ska ge akt på ändringar i denna lag och i Tillståndsmyndighetens föreskrift och justera driftmiljön i enlighet med ändringarna. Väsentliga förändringar i driftmiljön ska anmälas till bedömningsorganet för informationssäkerhet eller certifieringsorganet. Bedömningsorganets eller certifieringsorganets intyg ska förnyas, om betydande förändringar görs i driftmiljön eller om minimikraven på driftmiljön har ändrats på ett sätt som förutsätter en förnyad bedömning.

— —

30 §

Övervakning och inspektioner av informationssystem

Tillstånds- och tillsynsverket för social- och hälsovården ska övervaka och främja att informationssäkra driftmiljöer uppfyller kraven på dataskydd och informationssäkerhet. Certifieringsorganen ska övervaka och främja att de driftmiljöer som de bedömt som informationssäkra uppfyller kraven på dataskydd och informationssäkerhet. Tillstånds- och tillsynsverket för social- och hälsovården för ett offentligt register över driftmiljöer som uppfyller kraven och som anmälts till verket.

— —

Tillstånds- och tillsynsverket för social- och hälsovården kan meddela närmare föreskrifter om övervakningen av informationssäkra driftmiljöer.

52 §

Publicering av resultat baserade på uppgifter utlämnade med stöd av ett dataanvändningstillstånd

— —

Tillståndsmyndigheten kan meddela närmare föreskrifter om säkerställande av anonymiseringen av de uppgifter som ska publiceras.

_____

Denna lag träder i kraft den 2022 . _____

Helsingfors den 2022

Statsminister

Sanna Marin

Familje- och omsorgsminister Aki Lindén