Informatieveiligheidscomité
Kamer sociale zekerheid en gezondheid

IVC/KSZG/24/114

BERAADSLAGING NR. 24/044 VAN 5 MAART 2024 MET BETREKKING TOT DE GOEDE PRAKTIJKEN DIE TOEGEPAST MOETEN WORDEN BIJ HET GEBRUIK VAN PUBLIEKE CLOUD DIENSTEN

Het informatieveiligheidscomité, kamer sociale zekerheid en gezondheid,

Gelet op de Verordening (EU) nr. 2016/679 van het Europees Parlement en de Raad van 27 april 2016 *betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG* (Algemene Verordening Gegevensbescherming of AVG);

Gelet op de wet van 30 juli 2018 *betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens*;

Gelet op de wet van 15 januari 1990 *houdende oprichting en organisatie van een Kruispuntbank van de Sociale Zekerheid*, in het bijzonder artikel 46;

Gelet op het rapport van de Kruispuntbank van de Sociale Zekerheid;

Gelet op het verslag van de voorzitter,

Beslist op 5 maart 2024, na beraadslaging, als volgt:

I. ONDERWERP VAN DE AANVRAAG

1. Organisaties en instellingen van sociale zekerheid kennen een groeiende noodzaak voor het gebruik van publieke cloud diensten. Bij het gebruik van deze diensten moet de verwerkingsverantwoordelijke erover waken dat de beveiliging van de informatie correct ingeregeld is, alsook dat de verwerkingen op die platformen conform de AVG gebeuren.

II. BEVOEGHEID

2. Krachtens artikel 46, § 1, van de wet van 15 januari 1990 *houdende oprichting en organisatie van een Kruispuntbank van de Sociale Zekerheid* kan de kamer sociale zekerheid en gezondheid van het informatieveiligheidscomité goede praktijken formuleren die het nuttig acht voor de uitvoering en de naleving van deze wet en haar uitvoeringsmaatregelen en van de door of krachtens de wet vastgestelde bepalingen tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens die de sociale zekerheid betreffen.

3. Het informatieveiligheidscomité acht zich bijgevolg bevoegd.

III. GOEDE PRAKTIJKEN

4. Rekening houdend met de principes van de Algemene Verordening Gegevensbescherming (AVG) en de bepalingen van de wet van 30 juli 2018 *betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens*, formuleert de kamer sociale zekerheid en gezondheid van het informatieveiligheidscomité de volgende praktijken die bij het gebruik van publieke cloud diensten minimaal moeten worden toegepast.

5. Krachtens artikel 5 van de AVG zorgt de verwerkingsverantwoordelijke ervoor dat persoonsgegevens, door het nemen van passende technische of organisatorische maatregelen, op een dusdanige manier worden verwerkt dat een passende beveiliging ervan gewaarborgd is, en dat zij onder meer beschermd zijn tegen ongeoorloofde of onrechtmatige verwerking en tegen onopzettelijk verlies, vernietiging of beschadiging (integriteit en vertrouwelijkheid). Deze maatregelen moeten een passend beveiligingsniveau verzekeren, rekening houdend enerzijds met de stand van de techniek ter zake en de kosten voor het toepassen van de maatregelen en anderzijds met de aard van de te beveiligen gegevens en de potentiële risico's.

6. Bij het opstellen van de lijst van goede praktijken wordt vertrokken van het principe dat de publieke cloud dienstenleverancier geen toegang mag hebben tot de informatie die verwerkt wordt op het platform. Dit wordt gerealiseerd met *confidential compute*, waarbij encryptie ervoor zorgt dat de dienstenleverancier geen toegang heeft tot leesbare gegevens en code zowel in het geheugen als in de rekenunit. Deze beveiligde omgeving wordt ook enclave genoemd.

7. Bij het gebruik van *confidential compute* moeten minstens de volgende voorwaarden gerespecteerd worden:

a. De publieke cloud dienstenleverancier mag geen toegang hebben tot de verwerkte informatie

i. “Data at rest” moeten beschermd zijn, mogen enkel binnen de beveiligde enclave worden gedecrypteerd en moeten opnieuw geëncrypteerd worden voordat ze de enclave verlaten.
ii. “Data in transit” moeten beschermd zijn, mogen enkel binnen een beveiligde enclave gedecrypteerd worden en moeten opnieuw geëncrypteerd worden voordat ze de enclave verlaten.
iii. Informatie mag niet leesbaar over cloud netwerken getransfereerd worden, ook niet binnen het platform dat door de gebruiker werd opgezet. Dit is dus ook van toepassing voor communicatie tussen twee servers binnen hetzelfde platform.
iv. De uitwisseling van informatie met het cloud platform moet beveiligd gebeuren.

b. Attestatie van confidential computing van het publieke cloud platform

i. Vooraleer de software gevoelige informatie verwerkt op het *confidential computing* platform, moet deze voldoende garanties hebben dat het platform de nodige garanties op beveiliging biedt. Dit gebeurt middels attestatie van de *confidential compute*.
ii. De attestatie moet het mogelijk maken om te verifiëren dat de uitvoeringsomgeving vertrouwd en echt is, moet gebeuren op een betrouwbare manier en moet ook beveiligd zijn. De attestatie moet kunnen uitgevoerd worden onafhankelijk van de publieke cloud dienstenleverancier.

c. Encryptiemiddelen en secrets

i. Encryptiesleutels en secrets worden beveiligd tot binnen de enclave en zullen de enclave nooit leesbaar verlaten.
ii. Encryptiesleutels en secrets worden beheerd op een systeem waartoe de publieke cloud dienstenleverancier geen toegang heeft.

d. Authenticatiemiddelen

i. Authenticatiemiddelen moeten op dezelfde manier behandeld worden als secrets.
ii. De publieke cloud dienstenleverancier heeft geen toegang tot het systeem dat de authenticatiemiddelen beheert of het systeem dat de authenticatie uitvoert.

iii. De publieke cloud dienstenleverancier heeft geen logische toegang tot de servers of de enclaves, ook niet met eigen authenticatiemiddelen.

e. Autorisatiemiddelen

i. De publieke cloud dienstenleverancier heeft geen toegang tot het systeem dat de autorisaties beheert.

f. Verwijderen van gegevens

i. De publieke cloud dienstenleverancier geeft de nodige garanties dat data effectief verwijderd wordt van de storage-systemen wanneer de gebruiker hiertoe de opdracht geeft en laat deze procedure regelmatig attesteren door een externe partij.

g. Bewaking van gebruikte technologie

i. De gebruiker moet met de publieke cloud dienstenleverancier een overeenkomst aangaan dat de gebruiker onmiddellijk wordt ingelicht van eventuele kwetsbaarheden van het platform of onderdelen ervan zodat de gebruiker gepaste maatregelen kan nemen om het risico te beperken.

h. Service level agreement

i. De relatie met de publieke cloud dienstenleverancier moet een service level agreement omvatten dat in voldoende mate de garanties biedt dat de publieke cloud dienstenleverancier gepast reageert op eventuele bedreiging die impact kan hebben op de bescherming van de informatie.

i. Toepasselijke regelgeving en geschillen

i. De contracten met de publieke cloud dienstenleverancier moeten worden aangegaan onder Belgisch recht of recht van een ander Europees land. Geschillen in verband met de AVG worden door de Belgische autoriteit voor gegevensbescherming behandeld.

8. Het informatieveiligheidscomité herinnert eraan dat krachtens artikel 9 van de wet van 30 juli 2018 *betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens* de verwerkingsverantwoordelijke de volgende maatregelen neemt bij de verwerking van genetische, biometrische of gezondheidsgegevens:

1° hij of, in voorkomend geval, de verwerker wijst de categorieën van personen die toegang hebben tot de persoonsgegevens aan waarbij hun hoedanigheid ten opzichte van de verwerking van de betrokken persoonsgegevens nauwkeurig wordt omschreven;

2° hij of, in voorkomend geval, de verwerker houdt de lijst van de aldus aangewezen categorieën van personen ter beschikking van de bevoegde toezichthoudende autoriteit;

3° hij zorgt ervoor dat de aangewezen personen door een wettelijke of statutaire verplichting, of door een evenwaardige contractuele bepaling ertoe gehouden zijn het vertrouwelijk karakter van de betrokken gegevens in acht te nemen.

Deze beraadslaging treedt in werking op 20 maart 2024.

Michel DENEYER
Voorzitter