To: 5.1.2e [5.1.2e @rivm.nl]
Cc: 5.1.2e [5.1.2e @rivm.nl]; 5.1.2e [5.1.2e @rivm.nl]; 5.1.2e [5.1.2e @rivm.nl]
From: 5.1.2e
Sent: Mon 2/8/2021 8:23:06 AM
Subject: RE: Data velden/tabellen afstemmen - link, toelichting en def.tijd wordt aangevuld [PSEUDONIMISERINGSOPLOSSING CIMS]
Received: Mon 2/8/2021 8:23:08 AM

Beste 5.1.2e collega's,

Hetzelfde zou dan gelden voor onderstaande. Hoewel ik het natuurlijk altijd waardeer om op de hoogte te zijn van de laatste stand van zaken, mocht mijn betrokkenheid (weer) gewenst zijn.

Groet,
5.1.2e

From: 5.1.2e < 5.1.2e @rivm.nl>
Sent: vrijdag 5 februari 2021 16:57
To: 5.1.2e < 5.1.2e @rivm.nl>; 5.1.2e < 5.1.2e @rivm.nl>; 5.1.2e < 5.1.2e @rivm.nl>; 5.1.2e < 5.1.2e @rivm.nl>; 5.1.2e < 5.1.2e @rivm.nl>; 5.1.2e < 5.1.2e @rivm.nl>
Cc: 5.1.2e < 5.1.2e @rivm.nl>; 5.1.2e < 5.1.2e @rivm.nl>; 5.1.2e < 5.1.2e @rivm.nl>; 5.1.2e < 5.1.2e @rivm.nl>; 5.1.2e < 5.1.2e @rivm.nl>; 5.1.2e < 5.1.2e @rivm.nl>; 5.1.2e < 5.1.2e @rivm.nl>
Subject: FW: Data velden/tabellen afstemmen - link, toelichting en def.tijd wordt aangevuld [PSEUDONIMISERINGSOPLOSSING CIMS]

Collega's,
Dank aan 5.1.2e voor het gesprek dat hij arrangeerde met 5.1.2e
Zeer nuttig, nu de pseudonimiseringsoplossing in CIMS (BI) én de PSA CIMS BI volop de aandacht hebben en er significante keuzes moeten worden gemaakt over de passendheid van de treffen IB en P maatregelen in BI – CIMS.

Het door 5.1.2e georganiseerde overleg met 5.1.2e statistisch onderzoeker bij het CBS over de pseudonimiseringsoplossingen bij het CBS was uiterst informatief. 5.1.2e heeft veel expertise en ervaring met het Stelsel van Sociaal-Statistische Bestanden (SSB) en deelde met ons enkele wetenswaardigheden rondom de pseusonimiseringsoplossing die het CBS hanteert. Ik probeer, voor wie niet bij dit gesprek kon zijn, het gesprek in het kort weer te geven.

- CBS beweegt zich (enkel) in het (AVG) domein van wetenschappelijk onderzoek en statistiek
- Kwesties als wettelijke grondslag en doelbinding liggen voor het CBS eenvoudiger dan bij het RIVM
- Leidend is het beginsel van dataminimalisatie
- Vaststelling van een acceptabele mate van herleidbaarheid van gegevens (onthullingsrisico) wordt gedaan door methodologen (methodologie afdeling)
- Wat kan worden beschouwd als acceptabele mate van herleidbaarheid is context afhankelijk (soort gegevens, soort verwerking, ernst van inbreuk op rechten en vrijheden burger)
- De verantwoordelijkheid voor het onthullingsrisico bij publicaties ligt bij de onderzoeker die het onderzoek publiceert
- Het CBS verwerkt grote hoeveelheid data: veel data van één persoon en data van veel personen. Data worden veelvuldig "doorgekoppeld".
- De pseudonimiseringsoplossing is een mix van technische en organisatorische maatregelen
- De wetenschappelijke eis van reproduceerbaarheid maakt dat er bij de keuze van de sleutel en de opslag van de bestanden (qua versie e.d.) rekening mee moet worden gehouden

Scheiding

- Er wordt gewerkt met een geïntegreerde data-omgeving. De omgeving waarin wel en niet met persoonsgegevens wordt gewerkt zijn gescheiden.
- Datasets zijn gescheiden
- Degenen die toegang hebben tot het centraal koppelbestand (BSN/RINnr), hebben geen toegang tot de centrale gegevensbibliotheek.
- Er wordt gewerkt met gescheiden accounts. Een voor wanneer je wel en een ander voor wanneer je niet met persoonsgegevens werkt.

Beperkte toegang

- er is een zeer beperkt aantal mensen (4 van de 3000 CBS medewerkers), dat toegang heeft tot de persoonsgegevens én het pseudo ID (RINnr.)
- toegang tot de omgeving waarin persoonsgegevens worden verwerkt, is enkel benaderbaar door middel van een zgn. datasluis (één weg in en uit)
- onderzoekers hebben geen rechtstreekse toegang tot de databibliotheek. Dat hebben speciaal daarvoor geautoriseerde medewerkers, zgn. satelliet coordinatoren.
- De omgeving waarin gewerkt wordt met persoonsgegevens is enkel benaderbaar door middel van een datakluis (speciale map op het netwerk voor im- en export vanuit die omgeving. Andere kanalen zijn dichtgezet (dropbox, mail, netwerkschijf enz.)

Logging & monitoring

- De bestanden die de datasluis passeren (im- en export), blijven in de datakluis staan, zodat er kan worden gemonitord welke verwerkingen er hebben plaatsgevonden. Toezichthouden hierop, is de taak van een speciaal daarvoor aangewezen persoon.

Auditing en certificering

- (Delen van) processen zijn gecertificeerd
- Er worden regelmatig (QA) audits uitgevoerd door externe auditors

Beperking koppel baarheid

- Beslist is (maar nog niet geïmplementeerd), dat er naast de generieke sleutel, ook gewerkt gaat worden met een onderzoeksspecifieke sleutel. Een nummer dat onderzoeksspecifiek is, zodat data (sets) niet onderling te koppelen zijn.

En hoe nu verder ?
5.1.2e zal dit verder brengen met zijn collega architecten, verwacht ik. Welke pseudonimiseringsoplossing passend is, in het kader van de AVG is m.n. afhankelijk van de context (verwerkingen).
In het kader van IB en P compliance, zal de pseudonimiseringsoplossing onderwerp moeten zijn van een risico-inventarisatie en verantwoording in het kader van de AVG (DPIA).
Voor de liefhebber voeg ik ter illustratie een voorbeeld (nog onder de Wbp), bij.

Ik verwacht dat we met vereende krachten zullen komen tot een adequate keuze en verantwoording van een door het RIVM te kiezen passende pseudonimiseringsoplossing.
Tot nadere toelichting ben ik vanzelfsprekend bereid.

Vr. groet,
5.1.2e

From: 5.1.2e
Sent: vrijdag 5 februari 2021 09:39
To: 5.1.2e < 5.1.2e @rivm.nl>; 5.1.2e < 5.1.2e @rivm.nl>; 5.1.2e < 5.1.2e @rivm.nl>; 5.1.2e < 5.1.2e @rivm.nl>
Cc: 5.1.2e < 5.1.2e @rivm.nl>; 5.1.2e < 5.1.2e @rivm.nl>; 5.1.2e < 5.1.2e @rivm.nl>; 5.1.2e < 5.1.2e @rivm.nl>; 5.1.2e < 5.1.2e @rivm.nl>
Subject: FW: Data velden/tabellen afstemmen - link, toelichting en def.tijd wordt aangevuld [PSEUDONIMISERINGSOPLOSSING CIMS]

Beste allemaal,

Het is goed te zien dat de pseudonimiseringsoplossing steeds concreter wordt.
De privacy professionals onder ons kijken er met de blik van de toezichthouder en wetgever naar.

Ik reageer even als privacy officer RIVM.
Bij de advisering van de PSA van BI- CIMS, brachten we (CIO-O & FCC) gezichtspunten in. Enkele daarvan breng ik graag onder jullie aandacht.
De heersende opvatting is dat bij het vast stellen of een gegeven een persoonsgegeven is, *de mate van herleidbaarheid* – beoordeeld naar state of the art maatstaven-
centraal staat en de vraag of (in)directe herleidbaarheid van binnen een verwerking met privacygevoelige gegevens *tot een acceptabel niveau gereduceerd wordt.*

Een voorbeeld.
Anonieme gegevens zijn gegevens die geen betrekking hebben op een geïdentificeerde of identificeerbare natuurlijke persoon
of persoonsgegevens die zodanig anoniem zijn gemaakt dat de betrokkene niet of niet meer identificeerbaar is.
In het kader van het wetsvoorstel Tijdelijke wet informatieverstrekking RIVM ivm COVID, oordeelt *de regering* dat gegevens anoniem zijn wanneer
gegevens zijn ontdaan van alle direct herleidbare informatie door ze te versleutelen en te voorzien van een nieuw ID (pseudonimisering)
en de gegevens in geaggregeerde vorm aan te bieden door totaalaantallen te verstrekken (en wanneer een totaal aantal lager is dan 15, wordt daar geen getal verstrekt,
Als extra maatregel). Het is overigens bekend dat het mogelijk is om in bepaalde gevallen toch deze gegevens tot een persoon te herleiden ook al lijkt dit weinig waarschijnlijk.

Niet altijd even makkelijk om de functionele eisen in de niet functionele eisen aan zo'n pseudonimiseringsoplossing te verbinden.

- **Privacy bevorderende oplossingen** de structuur van het informatiesysteem en de (wettelijke) eisen aan de gegevensverwerking bepalen de (functionele) eisen aan de toepassing van de privacy bevorderende technologie. Procedurele en organisatorische maatregelen maken ook onderdeel van die oplossing uit.
- **De (effectiviteit van) privacy bevorderende maatregelen** wordt bepaald door de juiste combinatie van aan de verwerking te stellen eisen én structuur van het informatie systeem en de functionele eisen aan de privacy bevorderende oplossing. Dit vergt inzicht aan de hand van een beschrijving van de voorgenomen gegevensverwerkingen uitgewerkt in een procesbeschrijving, datamodel/ dataflows/ datasets en systeemdecompositie om de effectiviteit van de maatrgelen en de passendheid (art. 32 AVG) van de pseudonimiseringsoplossing te beoordelen.
- **Pseudonimisering gezien vanuit de Autoriteit Persoonsgegevens:** er kan op verschillende manieren worden voldaan aan de eisen die de AVG stelt aan het pseudonimiseren van gegevensverwerkingen. Van geval tot geval moet worden beoordeeld welke combinatie van maatregelen als passend kan worden beschouwd. De vraag of het bijvoorbeeld mogelijk moet zijn om terug te kunnen naar de identificerende gegevens of juist niet, is een vraag die in dit kader gesteld moet worden. Op basis van de verwerkingsgrondslag, de aard van de verwerking en de daaraan verbonden risico's, kan de afweging worden gemaakt tussen het beoogde detail, mate van herleidbaarheid van de te verwerken gegevens, de impact op de persoonlijke levenssfeer van betrokkenen en de maatregelen om de risico's te mitigeren.
- **Pseudonimiseringsoplossing verwerkingen client- en vaccinatiegegevens CIMS** [optelsom van eisen aan gegevensverwerking en structuur/kenmerken informatiesysteem] De keuze van de pseudonimiseringsoplossing zal in elk geval zodanig dienen te zijn:

  - dat naar algemeen geldende maatstaven (state of the art) de (in)directe herleidbaarheid van binnen een verwerking met privacygevoelige gegevens *tot een acceptabel niveau gereduceerd wordt.* De beoordeling kan

het beste worden gedaan in de vorm van een gegevensbeschermingeffectbeoordeling, of Data Protection Impact Assessment (DPIA).
- er op basis van de verwerkingsgrondslag, de aard van de verwerking en de daaraan verbonden risico's, gedocumenteerd en beargumenteerd de afweging gemaakt tussen het beoogde detail, de mate van herleidbaarheid van de te verwerken gegevens, de impact op de persoonlijke levenssfeer van betrokkenen en de maatregelen om de risico's te mitigeren.
- er aantoonbaar, juist en actief geavanceerde privacybeschermende technieken worden ingezet
- het gevolgde proces (van pseudonimisering) en de daarbij geldende afspraken op transparante wijze is beschreven

Aanknopingspunten voor de keuze van een passende pseudonimiseringsoplossing: zie bijgevoegd concept toetsingskader pseudonimisering, waarin ik aan de hand van diverse publicaties, beslissingen AP en andere relevante bronnen, de verschillende topics heb samengebracht voor een te maken keuze van een passende pseudonimiseringsoplosisng.

Voor CIMS geldt in het bijzonder dat de nu al door de Autoriteit Persoonsgegevens opgeworpen vraag over pseudonimisering afdoende geadresseerd dient te worden, blijkend uit een AVG conforme pseudonimiseringsoplossing.

Tot nadere toelichting ben ik vanzelfsprekend bereid.
Een cc van deze mail stuur ik naar mijn collega 5.1.2e, sinds 1 februari Privacy Coördinator DVP. En naar 5.1.2e, 5.1.2e

Vr. groet,
5.1.2e

From: 5.1.2e <5.1.2e@rivm.nl>
Sent: donderdag 4 februari 2021 19:56
To: 5.1.2e <5.1.2e@rivm.nl>; 5.1.2e <5.1.2e@rivm.nl>; 5.1.2e <5.1.2e@rivm.nl>; 5.1.2e <5.1.2e@rivm.nl>
Cc: 5.1.2e <5.1.2e@rivm.nl>; 5.1.2e <5.1.2e@rivm.nl>; 5.1.2e <5.1.2e@rivm.nl>; 5.1.2e <5.1.2e@rivm.nl>
Subject: RE: Data velden/tabellen afstemmen - link, toelichting en def.tijd wordt aangevuld

d
Beste mensen,

Bijgaand zoals afgesproken de uitgewerkte lijst per veld voor pseudonimisering. Het is best een uitgebreide lijst. De pseudonimisering wordt het eerst toegepast op de ODS-tabellen. In deze tabellen wordt de informatie uit CIMS het eerst geïmporteerd. De BDS-tabellen zijn hiervan afgeleid. Ik heb geprobeerd consistent te zijn door dezelfde gegevens in beide soorten tabellen gelijk te labelen.

Graag jullie inhoudelijk oordeel hierover. 5.1.2e vraag aan jou om dit grondig te controleren.

Hierna moet ik nog kijken naar de functionele vraag die gesteld is: punt 2 op de agenda voor ons overleg van vanmorgen. Voor vanavond sluit ik echter af.

Inhoudelijk punt hiernaast is de overname van de gepseudonimiseerde gegevens van niet-gevaccineerden. Dit is waardevol om noemergetallen vast te stellen voor diverse te monitoren gegevens.

Met vriendelijke groet,

5.1.2e
Rijksinstituut voor Volksgezondheid en Milieu
Ministerie voor Volksgezondheid, Welzijn en Sport
A. van Leeuwenhoeklaan 9 | 3721 MA | Bilthoven
Postbus 1| 3720 BA Bilthoven
5.1.2e

E: 5.1.2e @rivm.nl

-----Oorspronkelijke afspraak-----
Van: 5.1.2e < 5.1.2e @rivm.nl>
Verzonden: vrijdag 29 januari 2021 08:24
Aan: 5.1.2e ; 5.1.2e ; 5.1.2e 5.1.2 5.1.2e
Onderwerp: Data velden/tabellen afstemmen - link, toelichting en def.tijd wordt aangevuld
Tijd: donderdag 4 februari 2021 10:00-11:00 (UTC+01:00) Amsterdam, Berlijn, Bern, Rome, Stockholm, Wenen.
Locatie: Webex

Overleg over de verwerking van de overige persoonsgegevens. Met name het detailniveau van geboortedatum en postcode moet afgestemd. Met 5.1.2e en 5.1.2e.

-- De volgende tekst niet verwijderen of wijzigen. --

Wanneer het tijd is, kunt u hier deelnemen aan uw Webex-vergadering.

Deelnemen aan vergadering

Meer manieren om deel te nemen:

Deelnemen via de vergaderingskoppeling

5.1.2e

Deelnemen via vergaderingsnummer

5.1.2e

Deelnemen met Microsoft Lync of Microsoft Skype voor Bedrijven

Kies 5.1.2e @lync.webex.com

Als u een host bent, klik dan hier om hostgegevens weer te geven.

Hulp nodig? Ga naar https://help.webex.com

•