**Vragen m.b.t. Memo Rapportage FG**

| Partij | Nr. | Vraag / Input | Antwoord / Reactie |
|---|---|---|---|
| **GroenLinks** | 1 | Er is besloten het register van verwerkingen niet extern te publiceren. Wat is de reden daarvoor? | Het intern publiceren van het register van verwerkingen heeft mede tot doel de kwaliteit ervan verder te verhogen. Vanzelfsprekend is het register door de privacy officers met grote zorgvuldigheid en in samenwerking met de procesverantwoordelijken gevuld. Het is echter aan de procesverantwoordelijken om ervoor te zorgen dat hun eigen processen juist en volledig zijn opgenomen. Dit wordt mogelijk gemaakt door het register doorlopend ter beschikking te stellen. Wanneer uit controles over een wat langere tijd blijkt dat de inhoud van het register juist en volledig is, is het streven om dit register ook extern openbaar te zetten. Wel met die aantekening dat in het register ook kwetsbaarheden van de provincie kunnen zijn opgenomen, bijvoorbeeld in de getroffen technische en organisatorische maatregelen. Het is niet wenselijke om dergelijke informatie extern te publiceren. |
| | 2 | In de rapportage wordt aangegeven dat in december 2020 een uitvraag is gedaan naar de hoog risico verwerkingen. Welke verwerkingen zijn er gerapporteerd? Zijn deze inmiddels beoordeeld of deze inderdaad hoog risico verwerkingen zijn, is naar alle hoog risico verwerkingen een DPIA uitgevoerd en in hoeverre is er sprake van hoge restrisico's? Wat is uw beleid ten aanzien hiervan? | In reactie op de genoemde uitvraag zijn processen aangedragen die een hoog risico bevatten op het gebied van privacy, bijvoorbeeld omdat zij bijzondere persoonsgegevens bevatten. Of een hoog bedrijfsrisico, zoals aanbestedingen met bedrijfsgevoelige informatie. De binnengekomen processen zijn allemaal beoordeeld op gevoeligheid en zo nodig ingepland voor een (uitgebreidere) risicoanalyse. Dat kan een DPIA zijn, maar ook een business impact analyse (BIA) of een andere vorm van risico-inschatting.<br>Vooralsnog zijn er geen DPIA's uitgevoerd waaruit een hoog restrisico volgt. Wanneer dat in de toekomst wel het geval is, zijn hierover procesafspraken om risico-acceptatie op het juiste niveau (het niveau van de verwerkingsverantwoordelijke) te laten plaatsvinden. Ook wordt het proces dan voorgelegd aan de Autoriteit Persoonsgegevens voor een voorafgaande raadpleging. |
| | 3 | Ten aanzien van de DPIA's geeft de FG aan dat er een aanzienlijke 'stocklist' ligt, maar er afgelopen jaar slechts enkele zijn uitgevoerd. Hoe staat het hier nu mee? In hoeverre lopen projecten of plannen risico op vertraging doordat gegevensverwerkingen niet tijdig beoordeeld zijn en daarom niet kunnen worden geëffectueerd? | Mede naar aanleiding van deze constatering is besloten om de uitvoering van DPIA's prioriteit te geven. Om de voortgang te bespoedigen is de coördinatie van de uitvoering ervan teruggelegd bij de privacy officer en wordt de Wasstraat slechts ingezet indien dit niet leidt tot vertraging.<br>Die DPIA's die betrekking hebben op projecten en processen die nog niet van start zijn werden al voortvarend opgepakt. Vertraging daarvan door te langdurige DPIA-projecten is mij niet bekend. Wel is het zo dat projectleiders in hun planning niet altijd rekening houden met een reële doorlooptijd van een DPIA. Het is daarom belangrijk dat een privacy officer tijdig bij een project wordt betrokken voor privacy advies. Dan kan – indien nodig – tijdig een DPIA worden uitgevoerd. De praktijk leert dat het nog wel eens voorkomt dat een privacy officer op het allerlaatste moment wordt gevraagd een DPIA uit te voeren. Dat er dan enige vertraging ontstaat bij de start van een project in onvermijdelijk. |

| | | | |
|---|---|---|---|
| **SGP** | 4 | We hebben dit stuk met instemming gelezen. We hebben hier twee vragen over:<br><br>Klopt het dat wij nog niet eerder hebben gehoord van de genoemde datalekken? Hoe ernstig waren deze lekken? | Deze datalekken zijn voorafgaand aan het verschijnen van de tussentijdse FG-rapportage niet gedeeld met PS. Dit omdat sprake was van een (zeer) beperkt organisatierisico. Dit blijkt ook uit het feit dat slechts in 2 gevallen melding bij de Autoriteit Persoonsgegevens is gedaan. Het merendeel van de datalekken betrof verkeerd verzonden mail of het gebruik van de cc in plaats van de bcc, waardoor mailadressen te breed toegankelijk waren. In de FG-jaarrapportage over 2021 zal meer inhoudelijke toelichting worden gegeven op de in dat kalenderjaar gemelde datalekken. Naar verwachting wordt deze jaarrapportage op 20 april besproken in de commissie BEM. Het college voert (vooralsnog) de lijn alle datalekken te verantwoorden bij de jaarrapportage, tenzij de beoordeling van de materialiteit van het datalek ons inziens noopt tot onmiddellijke melding aan PS. Zo ontving u van ons recent wel direct een schrijven rondom een kwetsbaarheid in JAVA Log4j. (zie memo bij 3.13 op uw agenda). Hier was en is geen sprake van een datalek (voor zover nu bekend), maar wel van een verhoogd risico. |
| | 5 | Worden alle aanbevelingen overgenomen? Zo ja, worden ze ook verwerking in het actiemanagement? | Dit betreft een ambtelijk stuk dat u naar aanleiding van een toezegging bij de bespreking van de kwartaalrapportage BV Beter en IEA over het derde kwartaal 2021 is toegestuurd. Zoals in de begeleidende memo aangekondigd krijgt u nog de jaarrapportage. Dit ambtelijk stuk is besproken in het Concern Managementteam en die waren akkoord met de aanbevelingen. Ze worden niet verwerkt in het actiemanagement. |