Reactie op advies FG VWS

Het advies van de FG bevat een aantal punten, die worden aangehaald om de risico's voor de verwerking beheersbaar te houden. Wij nemen de adviezen van de FG onverkort.
Per punt leggen we uit hoe vorm wordt gegeven aan de invulling hiervan:

1. *Beveiliging van de backend*
   Highlights van de beveiligingsmaatregelen aan de backend server:
   a. Verificatie op basis van een penetratietest.
   b. Verificatie op basis van een review van de broncode.
   c. Procedurele audit op de backend gericht op procedures en de configuratie.
   d. Actieve monitoring op aanvallen.
   e. Het ontdoen van de DK's van het IP-adres van de verzender om herleidbaarheid te voorkomen.
   f. TEKs worden pas een DK na tijdig ontvangst van een cryptografische code via de GGD.
   g. Het scheiden van de omgeving om TEKs te uploaden en DKs te publiceren.
   h. Zeer korte bewaartermijnen om de impact van inbreuken te beperken.

2. *Niet alleen in het traject naar de livegang toe moeten tests worden uitgevoerd, maar ook na de livegang moeten verificatieslagen worden uitgevoerd:*
   a. De bestelde penetratietest van week 29 wordt uitgevoerd als nulmeting, er is wordt een aanvullende test besteld na livegang om het geheel nogmaals te testen. Er wordt dan een dubbele slag uitgevoerd. De laatste slag wordt agressief ingestoken (red teaming).
   b. Er wordt een responsible disclosure/coordinated vulnerability disclosure opgezet, waardoor melders worden beloond voor het doen van meldingen.
   c. Na een eventuele relevante update van app of backend zal een nieuwe penetratietest worden uitgevoerd door een andere partij dan de huidig aangezochte partij.

3. *Aanvullende of aangepaste DPIA voor internationale samenwerking.*
Voor internationale samenwerking komt een aanvullende DPIA die zal worden voorgelegd aan de FG.

4. *Evaluatie app*
Conform advies van de FG zal de evaluatie van de app ingericht worden zodat de effectiviteit periodiek wordt geëvalueerd. Uitgangspunt hierbij is dat hier geen identificerende gegevens vanuit de app worden verwerkt. De voorgenomen uitwerking wordt voorgelegd aan de FG.

Wij nemen daarmee alle adviezen van de Functionaris voor de Gegevensbescherming ter harte.