Het Logboek Dataverwerkingen en de risico's

Bij de implementatie en het beheer van het Logboek Dataverwerkingen is het van belang een analyse uit te voeren ten aanzien van (beveiligings-)risico's en, indien nodig, passende maatregelen te nemen. Ongeautoriseerde inzage en diefstal van data kunnen grote (maatschappelijke) gevolgen hebben. Dus naast de beveiliging van de applicatie die gevoelige data verwerkt, moet er ook nagedacht worden over de beveiliging van het logboek waarin verwerkingsactiviteiten worden gelogd.

Het doel van dit document is een voorbeeld aan te reiken ten aanzien van het opstellen en uitvoeren van een risicoanalyse ten behoeve van het implementeren en beheren van een Logboek Dataverwerkingen. Het uitgewerkte voorbeeld is niet bedoeld als standaard, wel geeft het een beeld van de risico's die van toepassing kunnen zijn bij de implementatie en beheer van een Logboek Dataverwerkingen.

Beleid vanuit de overheid

Vanuit de overheid zijn er diverse initiatieven ontwikkeld om risico's in kaart te brengen. Een belangrijke en wellicht de bekendste risicoanalyse is de Baseline Informatiebeveiliging Overheid (BIO). De Baseline Informatiebeveiliging Overheid (BIO) is het basisnormenkader voor informatiebeveiliging binnen alle overheidslagen (Rijk, gemeenten, provincies en waterschappen). Een ander voorbeeld is de Handreiking Diepgaande Risicoanalyse Methode Gemeenten en Handreiking Risicomanagement voor digitale weerbaarheid van departement-overstijgende ketens.

In sommige gevallen moet een diepere risicoanalyse worden uitgevoerd. De BIO onderscheidt drie basisbeveiligingsniveaus (BBN's). Ieder BBN bestaat uit een aantal controls, een aantal verplichte overheidsmaatregelen en een verantwoordings- en toezichtregime. Elk niveau bouwt voort op het vorige niveau. Daarbij vult BBN2 de controls van BBN1 aan. BBN2 vult ook de overheidsmaatregelen van BBN1 aan of vervangt deze door maatregelen met meer gewicht. Hetzelfde geldt voor BBN3 in relatie tot BBN1 en BBN2. Op basis van een resulterende BBN kan er een diepere risicoanalyse nodig zijn. Meer informatie over de BBN's is te vinden in de Baseline Informatiebeveiliging Overheid (BIO).

Deze situaties waarin een diepere risicoanalyse nodig is, worden hieronder kort toegelicht.

DPIA: Data Protection Impact Assessment

Als een organisatie van plan is om persoonsdata te verwerken met een hoog privacy risico, dan is het verplicht een DPIA uit te voeren. Een DPIA is een instrument om vooraf de privacy risico's van een dataverwerking in kaart te brengen. Zodat de organisatie maatregelen kan nemen om deze risico's te verkleinen. Een DPIA moet worden uitgevoerd als er voldaan wordt aan één of meer soorten dataverwerkingen van een lijst van negen gedefinieerde soorten dataverwerkingen. Met een DPIA pre-scan kan bepaald worden of een DPIA nodig is.

Leg de bevindingen schriftelijk vast in een DPIA-rapport, die wordt opgesteld door middel van het Rapportagemodel DPIA.

DTIA: Data transfer impact assessment

Als persoonsgegevens doorgegeven worden naar een land buiten de Europese Economische Ruimte en het gebruikte doorgiftemechanisme op basis van artikel 46 AVG niet gebaseerd is op een adequaatheidsbesluit (bijvoorbeeld als gebruik gemaakt wordt van standard contractual clauses (SCCs)), is het noodzakelijk om een zogenoemde data transfer impact assessment (DTIA) uit te voeren. Het is aan te raden om de DTIA als bijlage op te nemen bij de DPIA en de genomen aanvullende technische maatregelen op te nemen bij vraag 17. Er is nog geen officieel model maar een representatief voorbeeld is de opslag van data bij AWS in de Verenigde Staten.

Rijksbreed cloudbeleid 2022

Indien gegevens opgeslagen of anderszins verwerkt worden in een publieke cloudvoorziening is daarop het cloudbeleid en het implementatiekader 'risicoafweging cloudgebruik' van toepassing.

Architectuur Digitale Overheid 2030

Het werkdocument 'Architectuur Digitale Overheid 2030' beschrijft de architectuur van de digitale overheid in 2030. Het geeft richting aan de ontwikkeling van de digitale overheid. Het document legt het fundament voor een verbindende architectuur van de digitale overheid. Het maakt verbindingen tussen overheidsorganisaties op alle bestuurslagen en hun architecturen.

In de context van een risicoanalyse, is vooral de paragraaf 7.1 Privacybescherming van belang. In deze paragraaf staan een aantal architectuurbouwstenen waaraan een applicatie moet voldoen. Deze eisen zijn ook genoemd in de bij deze handreiking geleverde voorbeeldrisicolijst. De bouwblokken zijn:

• Verplichte uitvoering van Data protection impact assessment (DPIA) wanneer persoonsgegevens door de overheid verwerkt worden. Als in de risicolijst de Betrouwbaarheidsaspecten (te) hoog zijn, moet een DPIA worden uitgevoerd.

• Privacy by design (in het ontwerp aandacht voor o.m. doelbinding, dataminimalisatie en afscherming van gegevens). Op basis van in losse projecten uitgewerkte bouwstenen zullen overheidsbrede Privacy Enhancing Technology bouwstenen ontstaan. In DreigingId 2 en 3 van de voorbeeldrisicolijst wordt aandacht besteed aan deze eis.

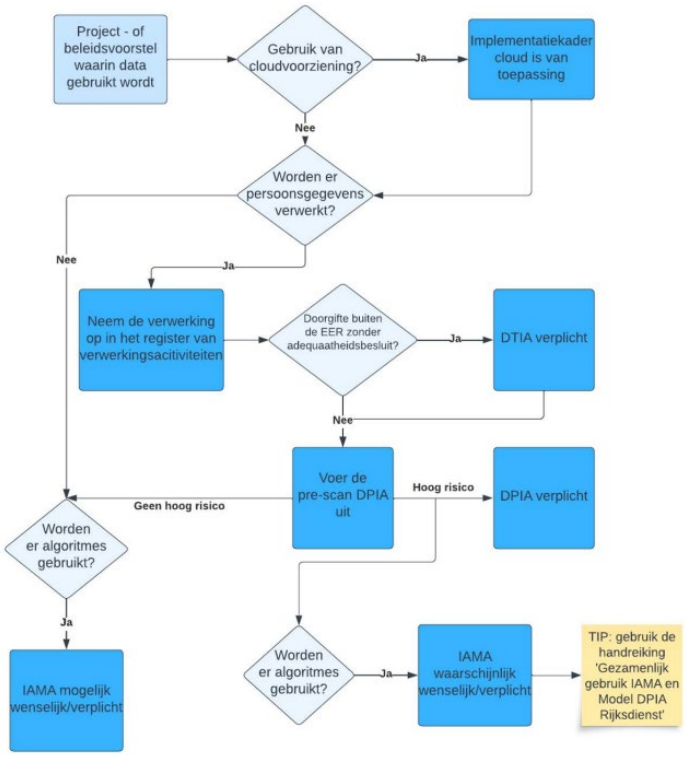
• Met organisaties of vertegenwoordigers die een bepaalde groep van belanghebbenden representeren, kunnen afspraken gemaakt worden over het delen van persoonsgegevens. In DreigingId 25 van de voorbeeldrisicolijst wordt aandacht besteed aan deze eis.

• BSNk is een bestaande bouwsteen om het BSN op privacy veilige manier om te zetten in een pseudoniem voor Toegangsvoorzieningen. In DreigingId 8, 43 en 44 van de voorbeeldrisicolijst wordt aandacht besteed aan deze eis.

• Logging en het voldoen aan transparantieverplichtingen vanuit Avg is een bouwsteen die generiek voor de hele digitale overheid geldt. Hier zijn diverse bouwstenen voor ontwikkeld. Meer hergebruik en standaardisatie is mogelijk en kan bijdragen aan de begrijpelijkheid en toegankelijkheid van deze oplossingen voor burgers. Implementatie van de Standaard Logboek Dataverwerkingen ondersteunt deze eis.

Wanneer welke risico-instrument toepassen?

Onderstaand stroomschema geeft aan op welk moment welk (diepte-) risicoanalyse-instrument uitgevoerd moet worden:



[Bron: Model DPIA Rijksdienst, Ministerie van Binnenlandse Zaken en Koninkrijkrelaties, mei 2023]

Opzet van het voorbeeld

De risicoanalyse in dit voorbeeld is qua opzet deels gebaseerd op de Handreiking Diepgaande Risicoanalyse Methode Gemeenten. Hierbij zijn ook de mogelijke maatregelen ten aanzien van een risico in een kolom opgenomen in plaats van deze apart uit te werken. De risico's die zijn genoteerd in de voorbeeldrisicoanalyse zijn bepaald door interne discussie waarbij vooral gelet is op de relevantie van de risico voor de implementatie en beheer van het Logboek Dataverwerkingen. In het voorbeeld is een subset van risico's bepaald op basis van de BIO-lijst, Handreiking Diepgaande Risicoanalyse Methode Gemeenten en eigen inzichten. Elke organisatie en applicatie is uniek, het is dus niet mogelijk om een uniform risicobeeld te schetsen voor de implementatie en beheer van het Logboek Dataverwerkingen. De uitwerking in dit voorbeeld is daarmee niet representatief voor elke situatie.

Het voorbeeld risicoanalyse is op een globaal niveau gedefinieerd, diepteanalyses (DPIA et cetera) zijn buiten beschouwing gelaten.

Gebruik van de risicolijst

Het staat elke organisatie vrij het voorbeeld aan te passen op de situatie ten behoeve van de implementatie en beheer van het Logboek Dataverwerkingen. Het is ten zeerste aan te raden om in ieder geval een risicoanalyse uit te voeren en maatregelen te implementeren indien nodig. Het model bestaat uit de volgende kolommen:

- **Component**: Categorie van bedreiging (deels afgeleid van de MAPGOOD-componenten zoals gebruikt in de Handreiking Diepgaande Risicoanalyse Methode Gemeenten).
- **DreigingId**: Uniek nummer van de geïdentificeerde dreiging.
- **Bedreiging**: Korte beschrijving van de bedreiging.
- **Betrouwbaarheidsaspect**: Het Betrouwbaarheidsaspect is een belangrijk onderdeel van de BIO-lijst.
- **Relevant voor LDV?**: Los van de beschreven scope van de het Logboek Dataverwerkingen, is het ook van belang voorwaardelijke zaken ten aanzien van de implementatie en beheer in ogenschouw te nemen zoals bijvoorbeeld toegangsbeveiliging.
- **Incidentgevolg**: Op basis van gedefinieerde teksten (tabblad 'Waarderingstabellen'), kan een mogelijk gevolg gekozen worden. De gedefinieerde teksten zijn bepaald op basis van de Handreiking Risicomanagement voor digitale weerbaarheid van departement-overstijgende ketens. Meerdere kolommen worden toegevoegd aan de referentietabel indien van toepassing.
- **Impact**: Een incident kan op verschillende manieren schade veroorzaken. De impact kan de organisatie raken maar ook de keten en derden. De gebruikte 5-puntsschaal is overgenomen van de 'Handreiking Risicomanagement voor digitale weerbaarheid van departement-overstijgende ketens'. De impact wordt automatisch bepaald op basis van het hoogste incidentgevolg (gekozen in de Íncidentgevolg' kolommen).
- **Kans**: Kans van optreden van de bedreiging. De gebruikte 5-puntsschaal is overgenomen van de Handreiking Risicomanagement voor digitale weerbaarheid van departement-overstijgende ketens.
- **Totaal**: Het product van Impact en Kans. Op basis van de gekozen Impact en Kans, wordt automatisch het risico geselecteerd uit de Risicomatrix die gedefinieerd is in het tabblad 'Waarderingstabellen'. De waarden in de Risicomatrix kunnen worden aangepast in het tabblad 'Waarderingstabellen'. De kleurcodes kunnen in de kolom zelf worden aangepast (voorwaardelijke opmaak).
- **Geaccepteerd risico**: Op basis van de uitkomst in de kolom 'Totaal' wordt er automatisch bepaald of het risico acceptabel is of niet. De waarden 'Geaccepteerd risico' kunnen worden aangepast in het tabblad 'Waarderingstabellen'.
- **Toelichting**: Indien gewenst kan er per bedreiging een toelichting worden gegeven.
- **Resultaat Baselinetoets BIO**: op basis van de gekozen waarde (L,M of H) per Betrouwbaarheidsaspect (B/I/V) wordt de juiste tekst automatisch geselecteerd uit het tabblad 'Waarderingstabellen'. Het resultaat kan zijn dat er in sommige gevallen een diepere analyse nodig is van het risico (DPIA).