Bijlage 1 – Checklist

Een Geb moet worden uitgevoerd wanneer een verwerking gelet op de aard, de omvang, de context of doelen ervan, waarschijnlijk een hoog risico voor de privacy van de geregistreerden oplevert. Of dat zo is moet de verantwoordelijke zelf bepalen. Om daarbij te helpen heeft de werkgroep van Europese privacy toezichthouders een lijst van negen criteria opgeleverd. Als de gegevensverwerking aan twee of meer van deze criteria voldoet, is het waarschijnlijk dat sprake is van een hoog risico en dient een Geb te worden uitgevoerd. Op de achtergrond spelen natuurlijk altijd de beginselen van proportionaliteit en subsidiariteit een rol.

Spelen twee of meer van de volgende criteria een rol bij de gegevensverwerking?

1. *Het beoordelen van mensen op basis van persoonskenmerken*

Ook wel profiling genoemd, het maken van prognoses en doen van voorspellingen op basis van kenmerken als persoonlijke voorkeuren, gedrag, enz. Een voorbeeld hiervan is het aanleggen van een bestand van bekende inbrekers en vervolgens op basis van kentekengegevens in ANPR hun reisbewegingen volgen om te voorspellen waar de volgende inbraak gaat plaatsvinden. Ook moet hierbij gedacht worden aan de ontwikkeling van risicotaxatie-instrumenten.

2. *Geautomatiseerde beslissingen*

Er wordt hierbij vooral gedoeld op beslissingen die voor de geregistreerde rechtsgevolgen hebben, gevolgen die zo wezenlijk zijn dat sprake is van uitsluiting of discriminatie. Geautomatiseerde besluitvorming is verboden, tenzij bij dergelijke beslissingen wordt voorzien in het recht op menselijke tussenkomst. [1]

3. *Stelselmatige en grootschalige monitoring*

Hier wordt gedoeld op monitoring in de openbare ruimte, bijvoorbeeld door middel van cameratoezicht (waaronder ANPR). Hierbij kunnen politiegegevens worden verzameld, zonder dat de geregistreerde weet wie die gegevens verzamelt en wat daar vervolgens mee gebeurt. Bovendien kan het onmogelijk zijn om je aan deze verwerking te onttrekken. Denk hierbij aan de CCTV camera's in steden, maar ook aan het monitoren van internetverkeer via webcrawlers

4. *Het verwerken van gevoelige gegevens, inclusief zeer persoonlijke gegevens*

Het gaat hierbij om bijzondere categorieën politiegegevens, zoals informatie over politieke voorkeur, seksuele geaardheid, biometrische gegevens, maar ook over gegevens die in het algemeen als privacygevoelig worden gezien, zoals gegevens omtrent elektronische communicatie, locatiegegevens en financiële gegevens.

5. *Grootschalige gegevensverwerkingen*

Er is niet direct een definitie van grootschalige gegevensverwerkingen en wanneer daarvan sprake zou zijn. De volgende criteria worden aangehouden om te bepalen of sprake is van een grootschalige gegevensverwerking:

- De hoeveelheid personen van wie gegevens worden verwerkt.
- De hoeveelheid en/of verscheidenheid aan gegevens die worden verwerkt.
- De tijdsduur van de gegevensverwerking.
- De geografische reikwijdte van de gegevensverwerking.

Denk hierbij aan Big Data-toepassingen, maar ook aan ANPR, dat zowel naar de hoeveelheid personen als naar de geografische reikwijdte is aan te merken als een grootschalige verwerking.

[1] Artikel 7a Wpg

6. *Koppelen en combineren van politiegegevens*

Het gaat hierbij om gegevensverzamelingen die aan elkaar gekoppeld of met elkaar gecombineerd zijn (in combinatie verwerken heet dat nu in de Wpg) waarvan de betrokkene dat redelijkerwijs niet zou verwachten. Denk bijvoorbeeld aan databases die voortkomen uit twee of meer verschillende gegevensverwerkingen met verschillende doelen, zoals het combineren van gegevens bij de Raffinaderij.

7. *Het verwerken van gegevens over kwetsbare personen*

Denk aan het verwerken van gegevens over minderjarigen of verwarde personen, maar ook aan oudere hulpbehoevende mensen of vluchtelingen. Bij het verwerken van dit type gegevens kan een Geb nodig zijn, omdat sprake is van een ongelijke machtsverhouding tussen de geregistreerde en de verantwoordelijke. Dit heeft tot gevolg dat de geregistreerde niet in staat wordt geacht in vrijheid toestemming te geven voor het verwerken van zijn gegevens. In de politie omgeving kun je hierbij denken aan Prokid (een systeem dat op basis van politieregistraties waarbij minderjarigen betrokken zijn, voorspellingen doet over crimineel gedrag op latere leeftijd.)

8. *Het gebruik maken van nieuwe technologieën*

Het gebruik van nieuwe technologieën kan gepaard gaan met nieuwe manieren om gegevens te verzamelen en gebruiken, met mogelijk grote privacyrisico's. Denk bijvoorbeeld aan ontwikkelingen rond sensing, zoals gezichts- of spraakherkenning en 'the internet of things'. Het gebruik maken van via die weg verzamelde gegevens kan een onverwacht grote impact hebben op het dagelijks leven en de privacy van mensen.

9. *Verwerkingen die leiden tot de blokkering van een recht, dienst of contract*

Het gaat hierbij om gegevensverwerkingen die ertoe leiden dat de geregistreerde een recht niet kan uitoefenen, een dienst niet kan gebruiken of een contract niet kan afsluiten. De discussies rond screening in het kader van autoverhuur of de verhuur van particuliere woningen zijn hier een voorbeeld van.

Er is sprake geweest van een 10e criterium: het delen van gegevens over de grenzen van de EU. Dit criterium is verdwenen, maar er dient wel rekening te worden gehouden met de staat van de privacybescherming in het ontvangende land, indien gegevens worden gedeeld buiten de EU. Mocht het zo zijn dat gegevens worden gedeeld met een niet EU land, waar de privacybescherming dusdanig slecht is dat een geregistreerde door de gegevensdeling een hoog risico loopt, moet dit in de overweging worden meegenomen.

Nee is niet aan de orde

Slotconclusie:

11.1