Cameratoezicht

Data Protection Impact Assessment

Datum	December 2022
Versie	1.0
Uitgevoerd door	Jeff van den Berg Privacy Officer

Data privacy impact assessment (DPIA)

Het (laten) uitvoeren van een DPIA kan de verantwoordelijke helpen om te voldoen aan voornoemde uitgangspunten en de toepasselijke wettelijke normen. Een DPIA is een hulpmiddel voor een verantwoordelijke om door middel van een vragenlijst de privacyrisico's van een (voorgenomen) verwerking in kaart te brengen. Aan de hand van een DPIA kan de verantwoordelijke de risico's beoordelen die de verwerking van persoonsgegevens door middel van een camera met zich meebrengt voor de rechten en vrijheden van de betrokkenen. Ook kan hij aan de hand van een DPIA maatregelen treffen om deze risico's te beperken. Hierdoor kan de verantwoordelijke de negatieve gevolgen die deze verwerking met zich mee kunnen brengen voor de betrokkenen, maar ook voor hemzelf, zo veel mogelijk beperken. Een DPIA is het meest doeltreffend als deze wordt uitgevoerd voordat een camera wordt ingezet. Ook als de omstandigheden met betrekking tot de inzet van een camera wijzigen (bijvoorbeeld een wijziging van de doeleinden of de omvang van het toezicht of hetgeen er met de camerabeelden zal worden gedaan), is het raadzaam om opnieuw een DPIA uit te voeren.
Vanuit de Algemene Verordening Gegevensbescherming (AVG) artikel 35 is het verplicht om in specifieke gevallen een Data Protection Impact Assessment (DPIA) uit te voeren
Dit document geeft invulling aan de DPIA voor SARKON, locatie: IKC de Driemaster, op basis van richtlijnen verkregen vanuit de Autoriteit Persoonsgegevens (AP).

Organisatie

SARKON is een katholieke organisatie en in 2001 ontstaan door een fusie van zeven schoolbesturen in de kop van Noord-Holland. Met de invoering van de nieuwe governancewet ging ook SARKON in 2011 over tot een scheiding van Bestuur en Toezicht. Nu bestaat de organisatie uit negentien katholieke basisscholen, waarvan twee interconfessioneel, in de kop van Noord-Holland, van Texel tot en met het zuiden van Hollands Kroon. De scholen worden bezocht door ongeveer 4100 leerlingen. SARKON heeft circa 425 medewerkers in dienst. Het bestuurskantoor staat in Den Helder. Daar zijn de bestuurders en stafmedewerkers werkzaam. Tevens wordt daar de volledige financiële- en personele administratie en ICT voor alle scholen uitgevoerd.

Scope en Aanleiding

Zeer frequent zijn en worden er rondom de school vernielingen aangericht als gevolg van vandalisme. Recent heeft er ook een inbraak plaatsgevonden. Dit heeft een omvangrijke schadepost qua materiaal en tijd met zich meegebracht.

Er is nagedacht of er minder ingrijpende onderzoeksmogelijkheden zijn om de onrechtmatige en/of strafbare gedraging aan het licht te brengen. Dat blijkt niet het geval te zijn.
Op basis van de voorgenomen maatregelen is de kans dat de risico's zich wezenlijk verkleinen. Daarom is besloten tot de inzet van cameratoezicht.

Het plaatsen van camera toezicht is in overleg gegegaan met de Gemeente(eigenaar van het pand), de politie, directie van de school, bevoegd gezag van Sarkon, privacy officer en de FG.
Het besluit zal tevens ter goedkeuring aan de MR van de school worden voorgelegd.

Sarkon heeft een cameraprotocol. Deze is verder leidend in hoe het camerasysteem verder wordt ingericht en welke afspraken er gemaakt moeten worden bij het uitlezen van de beelden.

Systeem en aansluiting

Het te leveren camerasysteem betreft:

- Hikvision IP netwerk recorder 4 kanalen 4K
- Harddisk 4TB
- Monitor 24 inch
- Power over Ethernet switch 5 poorten
- 3 xHikvision Colorvu Turret camera

SarkonICT (Netwerkbeheer) zorgt na de aanleg van het camerasysteem voor de aansluiting in het aanwezige netwerk. Er worden geen internet poorten opengezet zodat het camerasysteem is verbonden met het internet, Hierdoor zijn de beelden niet anders dan op de locatie uit te lezen, ook is dan gegarandeerd dat de opgenomen beelden lokaal zijn opgeslagen. De monitor en recorder worden geplaatst in een afsluitbare kast in en afsluitbare ruimte.
De directeur zal verder volgens het camera protocol handelen.
In afstemming met de directie van de school zal er een opnameschema worden opgesteld en vastgelegd.

Beslisregels

De vuistregel hiervoor is dat het uitvoeren van een DPIA noodzakelijk is wanneer de verwerking voldoen aan 2 of meer van onderstaande 9 criteriapunten. Per criteriapunt is in onderstaande tabel aangegeven of dit van toepassing is op de organisatie.

Criteria	Van toepassing op [BEDRIJFSNAAM]?	Onderbouwing
1. **Beoordelen van mensen op basis van persoonskenmerken**	Nee	
2. **Geautomatiseerde beslissingen**	nee	
3. **Stelselmatige en grootschalige monitoring**	Ja	Het gaat hierbij om monitoring van openbaar toegankelijke ruimten, bijvoorbeeld met cameratoezicht. Hierbij kunnen persoonsgegevens worden verzameld zonder dat betrokkenen weten wie hun gegevens verzamelt en wat daar vervolgens mee gebeurt. Bovendien kan het onmogelijk zijn voor mensen om zich in openbare ruimtes aan deze gegevensverwerking te onttrekken.
4. **Gevoelige gegevens**	Ja	Het gaat hierbij om bijzondere categorieën van persoonsgegevens (zie artikel 9 van de AVG), zoals informatie over iemands politieke voorkeuren. Ook strafrechtelijke gegevens vallen hieronder. Tot slot gaat het hier ook om gegevens die over het algemeen als privacygevoelig worden beschouwd, zoals gegevens over elektronische communicatie, locatiegegevens en financiële gegevens
5. **Grootschalige gegevensverwerkingen**	Nee	
6. **Gekoppelde databases**	nee	Lokale opslag
7. **Gegevens over kwetsbare personen**	Nee	
8. **Gebruik van nieuwe technologieën**	Ja	De AVG is er duidelijk over dat een DPIA nodig kan zijn bij het gebruik van een nieuwe technologie. De reden hiervoor is dat dit gebruik gepaard kan gaan met nieuwe manieren om gegevens te verzamelen en gebruiken, met mogelijk grote privacyrisico's.
9. **Blokkering van een recht, dienst of contract**	Nee	

Tabel 1: Criteriapunten uitvoeren DPIA

Afgaande op bovenstaande criteria, is het voor SARKON verplicht om een DPIA uit te voeren. Daarnaast heeft de AP heeft een lijst gepubliceerd conform artikel 35 lid 4 (zie bijlage 2) waarvoor het uitvoeren van een DPIA altijd verplicht is. Deze lijst wordt in tabel 2 tevens doorlopen, voor meer informatie wordt er verwezen naar bijlage 2. Indien het type verwerking van toepassing wordt geacht, wordt in de derde kolom een onderbouwing gegeven.

Type verwerking	Van toepassing	Onderbouwing
1. **Heimelijk onderzoek**	Nee	
2. **Zwarte lijsten**	Nee	
3. **Fraudebestrijding**	Nee	
4. **Creditscores**	Nee	
5. **Financiële situatie**	Nee	
6. **Genetische persoonsgegevens**	Nee	
7. **Gezondheidsgegevens**	Nee	
8. **Samenwerkingsverbanden**	Nee	
9. **Cameratoezicht**	Ja	Stelselmatige en grootschalige monitoring van openbaar toegankelijke ruimten met behulp van camera's
10. **Flexibel cameratoezicht**	Nee	
11. **Controle medewerkers**	[Nee	
12. **Locatiegegevens**	Nee	
13. **Communicatiegegevens**	Nee	
14. **Internet of Things**	Nee	
15. **Profiling**	Nee	
16. **Observatie en beïnvloeding van gedrag**	Nee	

Tabel 2. Lijst AP verplicht uitvoeren DPIA.

Uitvoer

Op basis van het document: “Richtsnoeren voor gegevensbeschermingseffectbeoordeling en bepaling of verwerking “waarschijnlijk een hoog risico inhoudt” in de zin van de Verordening 2016/679” geschreven door WP29 is onderstaand stappenplan vormgegeven. Punt 7 is toegevoegd om de PDCA cyclus beter te doorlopen:

1. Beschrijving van de (beoogde) verwerking
2. Beoordeling van de noodzaak en evenredigheid
3. Beoogde maatregelen om naleving aan te tonen
4. Beoordeling van de risico’s voor de rechten en vrijheden
5. Beoogde maatregelen om de risico’s aan te pakken
6. Documentatie
7. Aandachtspunten
8. Toezicht en evaluatie

Beschrijving van de (beoogde) verwerking	*Beschrijven van de verwerking waarbij o.a. de volgende punten aan bod komen:* ● *Doel van de verwerking* ● *Omvang van de verwerking* ● *Omschrijving van de gegevens die verwerkt worden* ● *Beschrijving van de verwerking die wordt uitgevoerd* ● *Wie er toegang hebben tot de gegevens* ● *Hoelang de gegevens worden bewaard en op wat voor locatie (hardware, software, netwerk, papier etc.)*	● *Doel van de verwerking* Beveiliging van het gebouw en de omliggende speelplaats ● *Omvang van de verwerking* ● *Omschrijving van de gegevens die verwerkt worden* ● *Beschrijving van de verwerking die wordt uitgevoerd* ● *Wie er toegang hebben tot de gegevens* zie Camera Protocol ● *Hoelang de gegevens worden bewaard en op wat voor locatie (hardware, software, netwerk, papier etc.* De opgenomen beelden worden automatisch na 6 weken gewist.
Beoordeling van de noodzaak en evenredigheid	*Beschrijf de rechtmatigheid van de verwerking (AVG artikel 6). Daarnaast beschrijven wat de noodzaak is om de gegevens te verwerken en of er bij de gegevensverwerking nagedacht is over dataminimalisatie (AVG artikel 5 lid 1c). Tevens het besluit ten aanzien van de bewaartermijn van de gegevens noteren (AVG artikel 5 lid 1e).*	De verwerking is noodzakelijk om de vitale belangen van de betrokkene of van een andere natuurlijke persoon en goederen te beschermen Zeer frequent zijn en worden er rondom de school vernielingen aangericht als gevolg van vandalisme. Recent heeft er ook een inbraak plaatsgevonden. Dit heeft een omvangrijke schadepost qua materiaal en tijd met zich meegebracht. Er is nagedacht of er minder ingrijpende onderzoeksmogelijkheden zijn om de onrechtmatige en/of strafbare gedraging aan het licht te brengen. Dat blijkt niet het geval te zijn. Op basis van de voorgenomen maatregelen is de kans dat de risico's zich wezenlijk verkleinen dat besloten is tot de inzet van cameratoezicht. De camera's worden gericht op de buitengebieden. er is geen sprake van cameratoezicht in het gebouw.

		Het plaatsen van camera toezicht is in overleg gegegaan met de Gemeente(eigenaar van het pand) , de politie, directie van de school en het bevoegd gezag van Sarkon. Sarkon wordt verantwoordelijk voor het verwerken van de opgenomen beelden. Het gebruik van het systeem zal tevens ter goedkeuring aan de MR van de school worden voorgelegd. Deze DPIA is daar onderdeel van. Sarkon heeft een cameraprotocol. Deze is verder leidend in hoe het camerasysteem verder wordt ingericht en welke afspraken er gemaakt moeten worden bij het uitlezen van de beelden.
Beoogde maatregelen om naleving aan te tonen	*Beschrijf wat de organisatie voor stappen heeft ondernomen om conform de AVG naleving aan te tonen.* *Denk hierbij aan:* ● *Informeren van betrokkene omtrent gegevensverwerking (bijvoorbeeld door informatie op website of patiënten folder) (AVG artikel 12 tot en met 14)* ● *Procedures vormgegeven rondom:* ○ *Inzage, rectificatie of verwijderen van gegevens.* ○ *Rechten van betrokkene (AVG artikelen 16 tot en met 21)* ● *Verwerkingsregister vormgegeven* ● *Verwerkersovereenkomsten met Verwerkers (AVG artikel 28)*	Alle ouders worden geïnformeerd middel een item in de nieuwsbrief. Op de ramen, deuren van het gebouw en langs de randen van de speelplaats worden borden geplaatst. Het systeem wordt zo ingericht dat er dagelijks van 17.00u - 8.uur. In de weekenden en vakanties de gehele dagen cameratoezicht is(beelden worden opgenomen) Alle beelden worden zoals het camera protocol beschrijft lokaal opgeslagen. Er vinden dus geen verdere verwerkingen plaats dan vermeld in het protocol.
Beoordeling van de risico's voor de rechten en vrijheden	*Kijk naar de (mogelijke) risico's voor de betrokkene. Geadviseerd wordt een risicoanalyse uit te voeren.*	zie tabel 3
Beoogde maatregelen om de risico's aan te pakken	*Geef een beschrijving van de maatregelen die de organisatie gaat treffen of al heeft getroffen. Dit op basis van de risicoanalyseg*	zie cameraprotocol

Documentatie	*Beschrijf welke documentatie reeds aanwezig is om bovenstaande zaken aan te tonen.*	zie cameraprotocol
Aandachtspunten	*Benoem de aandachtspunten die voortkomen uit het kritisch bekijken en beschrijven van het bedrijfsproces. Aandachtspunten kunnen tevens voortkomen uit de risicoanalyse.*	Sarkon is zich bewust van de aandachtspunten en risico's. Door het protocol te hanteren worden deze risico's verkleind.
Toezicht en evaluatie DPIA	*Beschrijf wat het standpunt is van de organisatie voor toezicht en evaluatie van de uitgevoerde DPIA. De AP adviseert om een DPIA zeker 1x in de drie jaar opnieuw uit te voeren mits de gegevensverwerking ongewijzigd blijft.*	Er is een DPIA uitgevoerd voor de plaatsing van het systeem, december 2022. In december 2025 wordt dit proces herhaald.

Tabel 3

Omschrijving van bedreiging	Kans van optreden	Gevolgen	Risico (kans x gevolg)	Risico inventarisatie (huidige situatie)	Risicobehandeling	Actie('s) m.b.t. risicobehandeling
Schenden van privacy recht	*groot*	Hinderlijk				

Bijlage 1. Criteria AP voor beoordeling privacyrisico

De Europese privacytoezichthouders hebben 9 criteria opgesteld om te beoordelen of uw voorgenomen verwerking van persoonsgegevens een hoog privacyrisico oplevert voor de betrokken personen. Als vuistregel kunt u hanteren dat u een DPIA moet uitvoeren als uw verwerking aan 2 of meer van de onderstaande 9 criteria voldoet.

1. Beoordelen van mensen op basis van persoonskenmerken

Het gaat hierbij onder meer om profiling en het maken van prognoses, met name op basis van kenmerken als iemands beroepsprestaties, economische situatie, gezondheid, persoonlijke voorkeuren of interesses, betrouwbaarheid of gedrag, locatie of verplaatsingen.

Voorbeelden hiervan zijn een bank die de kredietwaardigheid van klanten bepaalt (creditscoring), een bedrijf dat DNA-testen aan consumenten levert om gezondheidsrisico's te testen en een bedrijf dat bezoekers van zijn website volgt en op basis daarvan profielen van deze mensen opstelt.

2. Geautomatiseerde beslissingen

Het gaat hierbij om beslissingen die voor de betrokkene rechtsgevolgen of vergelijkbare wezenlijke gevolgen hebben. Zo'n gegevensverwerking kan er bijvoorbeeld toe leiden dat mensen worden uitgesloten of gediscrimineerd. Gegevensverwerkingen met geringe of geen gevolgen voor mensen vallen niet onder dit criterium.

Voor meer informatie, zie de (Engelstalige) guidelines over profiling van de Europese privacytoezichthouders.

3. Stelselmatige en grootschalige monitoring

Het gaat hierbij om monitoring van openbaar toegankelijke ruimten, bijvoorbeeld met cameratoezicht. Hierbij kunnen persoonsgegevens worden verzameld zonder dat betrokkenen weten wie hun gegevens verzamelt en wat daar vervolgens mee gebeurt. Bovendien kan het onmogelijk zijn voor mensen om zich in openbare ruimten aan deze gegevensverwerking te onttrekken.

4. Gevoelige gegevens

Het gaat hierbij om bijzondere categorieën van persoonsgegevens (zie artikel 9 van de AVG), zoals informatie over iemands politieke voorkeuren. Ook strafrechtelijke gegevens vallen hieronder. Tot slot gaat het hier ook om gegevens die over het algemeen als privacygevoelig worden beschouwd, zoals gegevens over elektronische communicatie, locatiegegevens en financiële gegevens.

5. Grootschalige gegevensverwerkingen

De AVG geeft geen definitie van 'grootschalige gegevensverwerkingen'. De Europese privacytoezichthouders adviseren om met de volgende criteria te bepalen of hiervan sprake is:

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

6. Gekoppelde databases

Het gaat hierbij om gegevensverzamelingen die aan elkaar gekoppeld of met elkaar gecombineerd zijn. Bijvoorbeeld databases die voortkomen uit twee of meer verschillende gegevensverwerkingen met verschillende doelen en/of uitgevoerd door verschillende verantwoordelijken, op een manier die betrokkenen niet redelijkerwijs kunnen verwachten.

7. Gegevens over kwetsbare personen

Bij het verwerken van dit type gegevens kan een DPIA nodig zijn omdat er sprake is van een ongelijke machtsverhouding tussen de betrokkene en de verantwoordelijke. Dit heeft als gevolg dat betrokkenen niet in vrijheid toestemming kunnen geven of weigeren voor het verwerken van hun gegevens. Het kan hierbij om bijvoorbeeld werknemers, kinderen en patiënten gaan.

8. Gebruik van nieuwe technologieën

De AVG is er duidelijk over dat een DPIA nodig kan zijn bij het gebruik van een nieuwe technologie. De reden hiervoor is dat dit gebruik gepaard kan gaan met nieuwe manieren om gegevens te verzamelen en gebruiken, met mogelijk grote privacyrisico's.

De persoonlijke en maatschappelijke gevolgen van het gebruik van een nieuwe technologie kunnen zelfs nog onbekend zijn. Een DPIA helpt de verantwoordelijke dan om de risico's te begrijpen en te verhelpen.

Sommige 'Internet of Things'-toepassingen bijvoorbeeld kunnen een grote impact hebben op het dagelijks leven en de privacy van mensen, waardoor hierbij een DPIA nodig is.

9. Blokkering van een recht, dienst of contract

Het gaat hierbij om gegevensverwerkingen die tot gevolg hebben dat betrokkenen:
een recht niet kunnen uitoefenen of;
een dienst niet kunnen gebruiken of;
een contract niet kunnen afsluiten.

Bijvoorbeeld een bank die persoonsgegevens verwerkt om te bepalen of zij een lening aan iemand willen verstrekken.

Verantwoordingsplicht

Let op: deze 9 criteria zijn een handreiking om in te schatten of u een DPIA moet uitvoeren. Ook als u aan slechts één of geen van deze criteria voldoet, moet u goed kunnen onderbouwen waarom u ervoor kiest om geen DPIA uit te voeren. Dit maakt onderdeel uit van de verantwoordingsplicht.

Bijlage 2. Criteria AP voor het uitvoeren van een verplichte DPIA

De Autoriteit Persoonsgegevens heeft een lijst van verwerkingen opgesteld waarvoor het uitvoeren van een DPIA verplicht is vóórdat u met verwerken begint.

Let op: Uw verwerking moet altijd voldoen aan de AVG. Als uw voorgenomen verwerking op deze lijst staat, zult u altijd moeten nagaan of u voor deze verwerking een geldige grondslag heeft. Heeft u geen geldige grondslag, dan mag u de persoonsgegevens niet verwerken ongeacht de uitkomsten van een eventuele DPIA.

Deze lijst is pas echt definitief na afstemming in Europees verband. Deze lijst kan dus nog wijzigen. Ook zal periodiek worden bekeken of de lijst moet worden aangepast.

Begrippen

In de lijst van soorten verwerkingen waarvoor een DPIA verplicht is, komen de begrippen 'grootschalig', 'systematisch' en 'stelselmatig' voor. Het begrip grootschalig is door de Europese privacytoezichthouders verder ingevuld.

Op Europees niveau zijn de begrippen 'systematisch' en 'stelselmatig' (nog) niet verder ingevuld. Waar in onderstaande lijst wordt gesproken over 'systematisch' of 'stelselmatig' moet u denken aan verwerkingen die volgens een bepaald systeem plaatvinden. Een verwerking van persoonsgegevens die is opgenomen in de systemen of in het beleid van de organisatie moet worden beschouwd als een systematische of stelselmatige verwerking. Gegevensverwerkingen die ad hoc of incidenteel plaatsvinden moeten niet beschouwd worden als systematische of stelselmatige verwerkingen.

AP-lijst van verwerkingen waarvoor DPIA verplicht is:

1. Heimelijk onderzoek

Grootschalige en/of systematische verwerkingen van persoonsgegevens waarbij informatie wordt verzameld door middel van onderzoek zonder dat de betrokkene daarvan vooraf op de hoogte te stellen. Bijvoorbeeld heimelijk onderzoek door particuliere recherchebureaus, onderzoek in het kader van fraudebestrijding en onderzoek op internet in het kader van bijvoorbeeld online handhaving van auteursrechten. Heimelijk cameratoezicht door werkgevers in het kader van diefstal- of fraudebestrijding door werknemers (bij deze laatste verwerking dient ook in incidentele gevallen een DPIA te worden uitgevoerd).

2. Zwarte lijsten

Verwerkingen waarbij persoonsgegevens betreffende strafrechtelijke veroordelingen en strafbare feiten, gegevens over onrechtmatig of hinderlijk gedrag (artikel 33, lid 4, aanhef en onder c, UAVG)of gegevens over slecht betalingsgedrag door organisaties of particulieren worden verwerkt en gedeeld met derden.

Bijvoorbeeld zwarte lijsten of waarschuwingslijsten, zoals deze bijvoorbeeld gebruikt worden door verzekeraars, horecabedrijven, winkelbedrijven, telecomproviders alsook zwarte lijsten die betrekking hebben op onrechtmatig gedrag van werknemers, bijvoorbeeld in de zorg of door uitzendbureaus).

3. Fraudebestrijding

Grootschalige en/of systematische verwerkingen van (bijzondere) persoonsgegevens in het kader van fraudebestrijding. Bijvoorbeeld fraudebestrijding door sociale diensten of door fraudeafdelingen van verzekeraars.

4. Creditscores

Grootschalige en/of systematische gegevensverwerkingen die leiden tot of gebruik maken van inschattingen van de kredietwaardigheid van natuurlijke personen, bijvoorbeeld tot uitdrukking gebracht in een creditscore.

5. Financiële situatie

Grootschalige en/of systematische verwerkingen van financiële gegevens waaruit de inkomens- of vermogenspositie of het bestedingspatroon van mensen valt af te leiden. Bijvoorbeeld overzichten van bankoverschrijvingen, overzichten van de saldi van iemands bankrekeningen of overzichten van mobiele- of pinbetalingen.

6. Genetische persoonsgegevens

Grootschalige en/of systematische verwerkingen van genetische persoonsgegevens. Bijvoorbeeld DNA-analyses ten behoeve van het in kaart brengen van persoonlijke kenmerken, bio-databanken.

7. Gezondheidsgegevens

Grootschalige verwerkingen van gegevens over gezondheid (bijvoorbeeld door instellingen of voorzieningen voor gezondheidszorg of maatschappelijke dienstverlening, arbodiensten, reïntegratiebedrijven, (speciaal)onderwijsinstellingen, verzekeraars, en onderzoeksinstituten) waaronder ook grootschalige elektronische uitwisseling van gegevens over gezondheid.

Let op: individuele artsen en individuele zorgprofessionals zijn op grond van overweging 91 van de AVG uitgezonderd van de verplichting een DPIA uit te voeren.

8. Samenwerkingsverbanden

Het delen van persoonsgegevens in of door samenwerkingsverbanden waarin gemeenten of andere overheden met andere publieke of private partijen bijzondere persoonsgegevens of persoonsgegevens van gevoelige aard (zoals gegevens over gezondheid, verslaving, armoede, problematische schulden, werkloosheid, sociale problematiek, strafrechtelijke gegevens, betrokkenheid van jeugdzorg of maatschappelijk werk) met elkaar uitwisselen. Bijvoorbeeld in wijkteams, veiligheidshuizen of informatieknooppunten.

9. Cameratoezicht

Stelselmatige en grootschalige monitoring van openbaar toegankelijke ruimten met behulp van camera's, webcams of drones.

10. Flexibel cameratoezicht

Grootschalig en/of systematisch gebruik van flexibel cameratoezicht. Bijvoorbeeld camera's op kleding of helm van brandweer- of ambulancepersoneel, dashcams gebruikt door hulpdiensten.

11. Controle werknemers

Grootschalige en/of systematische verwerking van persoonsgegevens om activiteiten van werknemers te monitoren. Bijvoorbeeld controle van e-mail en internetgebruik, GPS-systemen in (vracht)auto's van werknemers of cameratoezicht ten behoeve van diefstal- en fraudebestrijding.

12. Locatiegegevens

Grootschalige en/of systematische verwerking van locatiegegevens van of herleidbaar tot natuurlijke personen. Bijvoorbeeld door (scan)auto's, navigatiesystemen, telefoons, of verwerking van locatiegegevens van reizigers in het openbaar vervoer.

13. Communicatiegegevens

Grootschalige en /of systematische verwerking van communicatiegegevens inclusief metadata herleidbaar tot natuurlijke personen, tenzij en voor zover dit noodzakelijk is ter bescherming van de integriteit en de veiligheid van het netwerk en de dienst van de betrokken aanbieder, of het randapparaat van de eindgebruiker.

14. Internet of things

Grootschalige en/of systematische verwerkingen door verantwoordelijken van persoonsgegevens die worden gegenereerd door apparaten die verbonden zijn met internet en die via internet of anderszins gegevens kunnen versturen of uitwisselen. Bijvoorbeeld ‘internet of things’- toepassingen, zoals slimme televisies, slimme huishoudelijke apparaten, connected toys, smart cities, slimme energiemeters, medische hulpmiddelen, etc.

15. Profilering

Systematische en uitgebreide beoordeling van persoonlijke aspecten van natuurlijke personen gebaseerd op geautomatiseerde verwerking (profilering). Bijvoorbeeld beoordeling van beroepsprestaties, prestaties van leerlingen, economische situatie, gezondheid, persoonlijke voorkeuren of interesses, betrouwbaarheid of gedrag.

16. Observatie en beïnvloeding van gedrag

Grootschalige verwerkingen van persoonsgegevens waarbij op systematische wijze via geautomatiseerde verwerking gedrag van natuurlijke personen geobserveerd, verzameld, vastgelegd of beïnvloed wordt, inclusief gegevens die voor het doel online behavioural advertising worden verzameld.

Bijlage 3. Voorbeeld Risicoanalyse [BEDRIJFSPROCES 1]

Omschrijving van bedreiging	Kans van optreden	Gevolgen	Risico (kans x gevolg)	Risico inventarisatie (huidige situatie)	Risicobehandeling	Actie(‘s) m.b.t. risicobehandeling
Schenden van privacy recht	*Klein*	*Ernstig*	*4 (Zie legenda, Klein is geclassificeerd als score 2, Ernstig is geclassificeerd als score 2)*			
Communiceren van gegevens met verkeerde persoon						
Onrechtmatige toegang tot gegevens						
Onrechtmatige wijziging van gegevens						
Onrechtmatige verwijdering van gegevens						
Identiteitsfraude						
Social engineering						
Recht op gegevenswissing niet uit kunnen voeren.						
Recht op inzage niet uit kunnen voeren.						
Recht op rectificatie niet uit kunnen voeren						

Legenda:

- **Kans van optreden:**
  1. Zeer klein (verwaarloosbare mogelijkheid van optreden)
  2. Klein (zou kunnen optreden, maar zal in vrijwel alle gevallen niet optreden)
  3. Middelmatig (mogelijk; optreden niet onwaarschijnlijk)
  4. Groot (zeer goed mogelijk; zal in een groot deel van de gevallen optreden)
  5. Zeer groot (zal zeker of vrijwel zeker optreden)

- **Gevolgen:**
  1. Hinderlijk (eenvoudig herstelbaar)
  2. Ernstig (moeilijk herstelbaar)
  3. Zeer ernstig (niet herstelbaar)
  4. Fataal
  5. Catastrofaal

Risicobehandeling

Voor de behandeling van de in deze analyse bepaalde risico's kunnen vijf scenario's worden genoemd:

1. vermijden van risico's door het aanpassen van bedrijfsprocessen en/of van de informatievoorziening;
2. overdragen van risico's aan andere partijen, bijvoorbeeld verzekeraars of leveranciers;
3. bewust aanvaarden van risico's;
4. verbeteren van huidige beheersmaatregelen;
5. opstellen van nieuwe beheersmaatregelen.

Bijlage 4: Cameraprotocol/cameratoezicht Sarkon

Cameratoezicht