

P.C.S.V.

Richtlijnen DPIA

Specifiek gericht op cameratoezicht.

Uitleg

Een DPIA is een Data Protection Impact Assessment.

Deze richtlijn beschrijft alles wat men over een DPIA moeten weten zodat deze juist uitgevoerd kan worden. Hierin is opgenomen waarom een DPIA uitgevoerd moet worden en in welke gevallen een DPIA vereist is. Tevens zijn uitzonderingen benoemd zodat ook duidelijk is wanneer een DPIA achterwege kan blijven, dat wil echter niet zeggen dat een DPIA in zo'n geval niet nuttig is.

Een DPIA is een middel om risico's op het gebied van gegevensverwerking en privacy in te schatten voordat een nieuwe verwerking van persoonsgegevens wordt gestart, of wanneer men een bestaande verwerking van persoonsgegevens aanpast.

De uitvoering van een DPIA kan door één iemand worden gedaan maar ook door meerdere personen, zolang zij allen bij de verwerking betrokken zijn. Tijdens de DPIA worden grofweg 4 aspecten van een verwerking beoordeeld:

- **de kenmerken van de verwerking;**
het doel van de verwerking, wie betrokken zijn en wat de verwerkingen betekenen voor de betrokkenen
- **de rechtmatigheid;**
de grondslag voor de verwerking en aan welke wet- en regelgeving je moet voldoen
- **de risico's** die kunnen optreden bij de verwerking;
zijn er mogelijk negatieve gevolgen voor de betrokkenen, is het waarschijnlijk dat die optreden en wat is de impact daarvan?
- **de maatregelen die je moet nemen** om die risico's zoveel mogelijk te beperken;
dekken die maatregelen de negatieve gevolgen af?

Als deze aspecten beoordeeld zijn dan wordt hier een verslag van gemaakt wat besproken wordt met de FG. Het oordeel van de FG hierin is leidend, als deze van mening is dat risico's niet afdoende zijn afgedekt dan moet er opnieuw gekeken worden hoe het wel kan. Als de FG akkoord is kan het bestuur vervolgens bij de besluitvorming betrokken worden.

Wanneer de verwerking is goedgekeurd kun je aan de slag met de verwerking. De verwerking moet ook worden genoteerd in het register van verwerkingen of het dataregister.

Deze richtlijn is gebaseerd op de handreikingen van Kennisnet, die gericht zijn op onderwijs. Een branche die in grote lijnen vergelijkbaar is met kinderopvang.

Standpunt AP:

Er zijn verschillende methodes om een data protection impact assessment (DPIA) uit te voeren. U kunt er zelf een kiezen, als u maar aan de basisvereisten voldoet zoals die in de AVG staan beschreven:

- *Een systematische beschrijving van de beoogde gegevensverwerkingen en de doeleinden hiervan. Beroept u zich op een gerechtvaardigd belang als grondslag voor de verwerking? Neem dit dan ook op in de beschrijving.*
- *Een beoordeling van de noodzaak en de proportionaliteit van de verwerkingen. Dat houdt in: is het verwerken van persoonsgegevens op deze manier noodzakelijk op uw doel te bereiken? En is de inbreuk op de privacy van de betrokkenen (de mensen van wie u gegevens verwerkt) niet onevenredig in verhouding tot dit doel?*
- *Een beoordeling van de privacyrisico's voor de betrokkenen.*
- *De beoogde maatregelen om (1) de risico's aan te pakken (zoals waarborgen en veiligheidsmaatregelen) en (2) aan te tonen dat u aan de AVG voldoet.*

Uitgangspunt DPIA

Een uitvoerige uitleg van het bovenstaande is te vinden via de volgende [link](#). Daar vind je een uitgebreide uiteenzetting over wat een DPIA is en vanuit welke gedachten een DPIA wordt uitgevoerd. De informatie uit de link is puur als extra achtergrond informatie bedoeld.

Hieronder volgt een voorbeeld van de te onderzoeken onderdelen van de verwerking die aan een DPIA wordt onderworpen.

1. Stap 1: Leg uit waarom een DPIA verplicht of gewenst is.

Leg in grote lijnen uit welk doel door het project beoogd wordt en wat voor soort verwerking dit inhoudt. Wellicht vindt u het handig om te verwijzen naar of te linken naar andere documenten, zoals een projectvoorstel. Vat samen waarom u de behoefte aan een DPIA hebt vastgesteld.

De Autoriteit Persoonsgegevens (AP) heeft een lijst van verwerkingen opgesteld waarvoor het uitvoeren van een data protect impact assessment (DPIA) altijd verplicht is vóór u met verwerken begint. Hier valt ook cameratoezicht onder.

Grootschalige verwerkingen en/of stelselmatige monitoring van openbaar toegankelijke ruimten met camera's.

Basisschool Gevers Deynoot heeft 2 camera's bij de entrees van de school hangen. In het verleden is er veel vandalisme geweest en pogingen tot inbraak. Dit is de reden dat er camera's zijn opgehangen.

2. Stap 2: omschrijf de verwerking

Beschrijf de aard van de verwerking: hoe gaat u gegevens verzamelen, gebruiken, opslaan en verwijderen? Wat is de bron van de gegevens? Worden de gegevens met derden gedeeld?
Tip: verwijs naar een stroomdiagram of een andere manier om gegevensstromen te beschrijven. Welke soorten verwerking waarvan is vastgesteld dat ze een hoog risico inhouden, zijn hierbij betrokken? Denk aan gevoelige of bijzondere persoonsgegevens?

Beschrijf hier het proces van de toegepaste cameratoezicht. Waarom is er toezicht, hoe worden de beelden opgenomen (techniek en stand camera's etc.). Op welke manier worden gegevens bewaard, opgeslagen en verwijderd enzo?

De beelden worden op een Stand-alone computer opgeslagen en zodra de schijf vol is, overschrijft deze de beelden automatisch. Er moet ingelogd worden om de beelden te bekijken en dit wordt alleen gedaan indien er noodzaak is. Dus bij inbraak of vandalisme. De camera neemt alleen beelden op als er beweging is, door de weeks is dat dus veel.

Openstaand: hoe lang duurt het voor dat de schijf wordt. Maximale opslagduur 1 maand

Elektrotechnisch bedrijf de Groot uit Voorschoten

Beschrijf de reikwijdte van de verwerking: wat is de aard van de gegevens en bevat deze speciale categorieën of strafbare feiten? Hoeveel gegevens verzamelt u en gebruikt u? Hoe vaak? Hoe lang worden ze bewaard? Hoeveel personen worden getroffen? Welk geografisch gebied dekt het?

Bij het maken van camerabeelden kunnen bijzondere persoonsgegevens op beeld komen te staan. Deze gegevens worden niet als bijzondere persoonsgegevens aangemerkt als:

- Het doel van het cameratoezicht is niet gericht op het vastleggen van de rasgegevens van de bezoekers, maar op beveiliging. Ook wordt middels het cameratoezicht geen onderscheid gemaakt op basis van het ras van de bezoekers.
- Het is voor de school redelijkerwijs niet voorzienbaar dat het cameratoezicht zal leiden tot het maken van onderscheid op basis van een bijzonder persoonsgegeven.
- Het verwerken van de rasgegevens van de bezoekers van de school is onvermijdelijk bij de inzet van cameratoezicht in een school.
- De verwerking van de camerabeelden heeft geen identificatie tot doel, tenzij er sprake is van een politieonderzoek.

De beelden worden alleen gebruikt bij de vandalisme, inbraak en als daar een gegronde toe is. Het hele schoolplein wordt gezien en alleen als er bewogen wordt, wordt dit opgenomen. De openbare weg is niet in beeld.

Beschrijf de context van de verwerking: wat is de aard van uw relatie met de betrokkenen? Hoeveel controle hebben zij over hun persoonsgegevens? Verwachten zij dat u hun gegevens op deze manier zou gebruikt? Gaat het om kinderen of andere kwetsbare groepen? Zijn er eerdere zorgen over dit type verwerking of zijn er reeds bekende beveiligingsfouten? Is het op geen enkele manier nieuw? Wat is de huidige stand van de technologie op dit gebied? Zijn er actuele zorgen van openbaar belang waar u rekening mee moet houden? Bent u aangemeld voor een goedgekeurde gedragscode of certificatieschema (nadat deze zijn goedgekeurd)?

Er worden beelden gemaakt van leerlingen, ouders, medewerkers en bezoekers.

Maak duidelijk aan de betrokkenen waar het cameratoezicht voor dient, en beschrijf hoe u dit aan hen hebt laten weten. Het is bij camera toezicht verplicht om dit bij de toegang tot het pand en/of gebied waar het toezicht plaatsvindt kenbaar te maken. Bijvoorbeeld een bordje waarop staat dat cameratoezicht plaatsvindt. Ook moeten camera's zichtbaar zijn geplaatst.

We hebben stickers op de deuren geplakt om kenbaar te maken dat er beveiligingscamera's zijn. Het cameraprotocol is ter inzage beschikbaar bij de conciërge of de directeur.

Beschrijf de doelen van de verwerking: wat wil je bereiken? Wat is het beoogde effect op individuen? Wat zijn de voordelen van de verwerking - voor u, en meer in het algemeen?

- de beveiliging van de toegang tot gebouwen en terreinen;
- de bewaking van zaken die zich aan de buitenkant van het gebouw of op het terrein bevinden;
- het vastleggen van incidenten.

Het ophangen van beveiligingscamera's ook als doel om af te schrikken, dat heeft hopelijk dus ook een preventieve werking.

3. Stap 3: Consulteren van betrokkenen

Overweeg hoe u relevante belanghebbenden kunt raadplegen: beschrijf wanneer en hoe u de opvattingen van individuele personen wilt opzoeken - of motiveer waarom het niet passend is om dit te doen. Wie moet je nog meer bij je organisatie betrekken? Moet u uw verwerkers vragen om te helpen? Bent u van plan om informatiebeveiligingsdeskundigen of andere deskundigen te raadplegen?

Uitvraag procedure bij de leverancier:

Stand alone computer en er moet ingelogd worden. De beelden zijn niet te vinden op internet

De leverancier doet ook het onderhoud.

4. Stap 4: beoordeel noodzakelijkheid en proportionaliteit

Beschrijf nalevings- en evenredigheidsmaatregelen, met name: wat is uw wettelijke basis voor verwerking? Bereikt de verwerking daadwerkelijk uw doel? Is er een andere manier om hetzelfde resultaat te bereiken? Hoe voorkomt u dat functies gaan kruipen? Hoe gaat u zorgen voor datakwaliteit en dataminimalisatie? Welke informatie geef je individuen? Hoe gaat u helpen om hun rechten te ondersteunen? Welke maatregelen neemt u om ervoor te zorgen dat de verwerkers hieraan voldoen? Hoe beschermt u internationale overschrijvingen?

Het cameratoezicht moet noodzakelijk zijn. Dat wil zeggen dat de onderwijsinstelling het doel niet op een andere manier kan bereiken. De onderwijsinstelling moet eerst nagaan of er geen andere mogelijkheid is, die minder ingrijpend is voor de privacy van betrokkenen. Ook mag het cameratoezicht niet op zichzelf staan. Het moet onderdeel zijn van een totaalpakket aan maatregelen in het kader van beveiliging en sociale veiligheid.

Concreet betekent het vorenstaande dat cameratoezicht ter beveiliging van personen en goederen slechts mag worden ingezet indien er ook andere beveiligingsmaatregelen zijn getroffen. Minder vergaande maatregelen dienen onvoldoende effectief te zijn en deze maatregelen kunnen redelijkerwijs niet worden uitgebreid. Tevens mogen er niet meer en langer camera's worden ingezet en niet meer personen en/of plaatsen in beeld worden gebracht dan strikt noodzakelijk is voor de gestelde doeleinden (dataminimalisatie). Dit betekent dat de verantwoordelijke alleen continu cameratoezicht mag instellen wanneer niet kan worden volstaan met opnames gedurende bepaalde periodes.

Naar aanleiding van diverse incidenten is besloten om over te gaan op cameratoezicht, het gaat vooral om incidenten buiten schooltijd en op het terrein. Het is voor de school anders niet mogelijk incidenten te monitoren. Binnen de school wordt niet gefilmd.

5. Stap 5: Identificeer en beoordeel risico's

Beschrijf de bron van het risico en de aard van de potentiële impact op individuen. Benoem indien nodig bijbehorende compliance- en bedrijfsrisico's.		Kans op schade Remote, possible or probable	Ernst van de schade Minimal, significant or severe	Algeheel risico Low, medium or high
R1	Ongeoorloofde inzage	Laag	Aanzienlijk	Laag
R2	Misbruik beeldmateriaal	Laag	Ernstig	Laag
R3	Technisch falen system	Laag	Minimaal	Laag
R4	Oneigenlijk gebruik door medewerkers en leidinggevenden	Laag	Minimaal	Laag

6. Stap 6: Benoem maatregelen om risico's te mitigeren

Identificeer aanvullende maatregelen die u zou kunnen nemen om risico's die als middelhoog of hoog risico zijn geïdentificeerd in stap 5, te verminderen of te elimineren.				
Risico	Maatregelen om risico te verminderen of te elimineren	Effect op risico	Rest risico	Maatregel goedgekeurd
		Geelimineerd Verminderd Acceptabel	Laag Medium Hoog	Ja/Nee
R1, R2	Beperkte toegang tot systemen middels een wachtwoord en codes, en eisen voor inzage in protocol vastgelegd.	verminderd	laag	Ja
R1, R2	Actie: Uitzocht geldende bewaartermijn. Beelden worden na maximaal 4 weken overschreven	Verminderd	Laag	Ja
R1, R2	Afspraken met personeel over geheimhouding, er komt een geheimhoudingsverklaring over geheimhouding.	Verminderd	laag	ja
R3	Stand alone computer wordt jaarlijks gecontroleerd en onderhouden door de leverancier.	geëlimineerd	laag	Ja
R4	Protocol cameratoezicht met afspraken medewerkers, goedgekeurd door MR van Gevers Deynoot en vastgesteld door bestuur.	Acceptabel	laag	ja
R4	Bezoekers zijn op de hoogte gesteld van het cameratoezicht. Er hangen stickers	Acceptabel	Laag	ja

7. Stap 7: Notuleer de uitkomst

Onderdeel	Naam/Datum	Opmerkingen
Maatregelen goedgekeurd door: FG	29 november 2022	Integreer acties in projectplan, met datum en verantwoordelijkheid voor voltooiing
Restrisico's goedgekeurd door:	Er zijn geen restrisico's aanwezig.	Neem contact op met de AP voordat u doorgaat met het accepteren van een hoog restrisico.
FG om advies gevraagd:	Ja,	De FG moet adviseren over compliance, de maatregelen en of de verwerking kan doorgaan.
Samenvatting van het advies van de FG: Cameratoezicht is goedgekeurd i.o.m. de GMR en vastgesteld door het bevoegd gezag		
Advies aanvaard of genegeerd door:		Als het advies genegeerd wordt moet dit worden verklaard.
Reactie op advies: N.v.t.		
Consultatiereacties beoordeeld door:		Als uw beslissing afwijkt van de mening van betrokkenen, moet u uw redenen uitleggen.
Uitleg: N.v.t.		
Deze DPIA zal worden beheerd en geëvalueerd door:	Evaluatie medio november 2024	De DPO moet ook de voortdurende naleving van DPIA evalueren