AVG Privacy document

Opdrachtgever: **Schietsportvereniging Veldhoven**
Projecteringsdeskundige CCTV: Jarno de Vroom
Opsteller: Jarno de Vroom

Inhoud:

Privacyverklaring

Schietsportvereniging Veldhoven respecteert de privacy van haar leden, in het bijzonder hun rechten met betrekking tot de verwerking van persoonsgegevens. Vanwege volledige transparantie hebben wij daarom een beleid geformuleerd en geïmplementeerd met betrekking tot deze verwerking zelf, het doel ervan alsook de mogelijkheden voor betrokkenen om hun rechten zo goed mogelijk te kunnen uitoefenen.

Voor alle aanvullende informatie over de bescherming van persoonsgegevens kunt u terecht op de website van de Autoriteit persoonsgegevens:
https://autoriteitpersoonsgegevens.nl/nl

De aan u beschikbaar gestelde privacy policy is de enige versie die van toepassing is, totdat een nieuwe versie de huidige versie vervangt.

Artikel 1 – Wettelijke bepalingen
Verantwoordelijke voor de verwerking van persoonsgegevens (Hierna ook “de beheerder”): Schietsportvereniging Veldhoven, correspondentieadres Borghoutspark 44, 5502 JZ Veldhoven, kvk-nummer: 40235141.

Artikel 2 – De verwerking van persoonsgegevens

1. Uw persoonsgegevens worden verzameld door Schietsportvereniging Veldhoven. Onder persoonsgegevens worden verstaan: alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon; als identificeerbaar wordt beschouwd een natuurlijk persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identificator zoals een naam, een identificatienummer, locatiegegevens, een online identificator of een of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit.

2. Wij verwerken de volgende categorieën gegevens van u:
   - Naam
   - Geslacht
   - Adresgegevens
   - E-mailadres(sen)
   - Telefoonnummer(s)
   - Geboortedatum / Leeftijd
   - Geboorteplaats
   - Verklaring Omtrent Gedrag
   - Uw naam en e-mailadres bij de baanreserveringen
   - Uw naam in het presentieregister
   - Uw naam op de munitiestaat
   - Uw naam in de wapenuitgiftelijst

Artikel 3 – Doel van de verwerking
We verzamelen uw persoonsgegevens niet zomaar. Uw persoonsgegevens worden verwerkt voor:

- Onze ledenadministratie
- Het voldoen aan de wettelijke verplichtingen
- De veiligheid op de schietbaan

Artikel 4 – Registratie persoonsgegevens
Uw persoonsgegevens worden geregistreerd in een (elektronisch) register.

Artikel 5 – Uw rechten met betrekking tot uw gegevens
Op grond van artikel 13 lid 2 sub b AVG heeft u recht op inzagen van en rectificatie of wisseling van uw persoonsgegevens of beperking van de u betreffende verwerking, alsmede het recht tegen de verwerking bezwaar te maken en het recht op gegevensoverdraagbaarheid. U kunt deze rechten uitvoeren door contact met ons op te nemen via secretaris@ssvveldhoven.nl.

Ieder verzoek daartoe dient te worden vergezeld door een kopie van een geldig identiteitsbewijs, waarop u uw handtekening heeft gezet en onder vermelding van het adres waarop er met u contact kan worden opgenomen. Binnen 1 maand na het ingediende verzoek, krijgt u antwoord op uw verzoek. Afhankelijk van de complexiteit van de verzoeken en het aantal van de verzoeken kan deze termijn indien nodig met 2 maanden worden verlengd.

Artikel 6 – Wettelijke verplichtingen
In geval van schending van enige wet- of regelgeving, waarvan u wordt verdacht en waarvoor de autoriteiten persoonsgegevens nodig hebben die de beheerder heeft verzameld, worden deze aan hen verstrekt na een uitdrukkelijk en gemotiveerd verzoek van die autoriteiten, waarna deze persoonsgegevens mitsdien niet meer onder de bescherming van de bepalingen van deze privacyverklaring vallen.

Artikel 7 – Commerciële aanbiedingen
U kunt commerciële aanbiedingen krijgen van de beheerder, wanneer u daar toestemming voor heeft gegeven. Indien u deze niet (meer) wenst te ontvangen, stuurt u een mail naar het volgende adres: secretaris@ssvveldhoven.nl
Uw gegevens worden niet gebruikt door partners van de verantwoordelijke voor commerciële doeleinden.

Artikel 8 – Bewaartermijn gegevens
De door de beheerder verzamelde gegevens worden gebruikt en bewaard voor de duur zoals deze bij wet is bepaald.

Artikel 9 – Toepasselijk recht
Op deze voorwaarden is Nederlands Recht van toepassing. De rechtbank van de vestigingsplaats van de beheerder is exclusief bevoegd bij eventuele geschillen omtrent deze voorwaarden, behoudens wanneer hierop een wettelijke uitzondering van toepassing is.

Artikel 10 – Contact
Voor verzoeken, vragen of meer informatie kunt u zich richten tot de secretaris van de vereniging, secretaris@ssvveldhoven.nl

Artikel 11 – Toepassing
Deze privacyverklaring is van toepassing sinds 5 augustus 2022 tot nader order

AVG en Cameratoezicht

Wat zegt de Autoriteit Persoonsgegevens over Cameratoezicht op verenigingen?

Cameratoezicht op de vereniging kan helpen tegen bijvoorbeeld diefstal of beschadiging van eigendommen. Maar de inbreuk op de privacy van de leden en bezoekers is groot. Daarom mogen besturen van verenigingen alleen camera's ophangen als zij aan een aantal voorwaarden voldoen.
Het bestuur moet ervoor zorgen dat de inbreuk op de privacy zo klein mogelijk is. Een camera in bijvoorbeeld een toilet of kleedhokje gaat te ver, omdat mensen dan bloot in beeld kunnen komen.
Verder mag de camera geen geluidsopnamen maken. Dit is voor het doel namelijk niet nodig.

Gerechtvaardigd belang
De vereniging moet een gerechtvaardigd belang hebben voor het cameratoezicht. Bijvoorbeeld diefstal tegengaan of leden en bezoekers beschermen.

Noodzaak cameratoezicht
Het cameratoezicht moet noodzakelijk zijn. Dat wil zeggen dat de vereniging het doel, bijvoorbeeld fraudebestrijding, niet op een andere manier kan bereiken. Is er geen andere mogelijkheid, die minder ingrijpend is voor de privacy? Dat moet de vereniging eerst nagaan. Ook mag het cameratoezicht niet op zichzelf staan. Het moet onderdeel zijn van een totaalpakket aan maatregelen.

Privacy toets
In dit document is een privacy toets opgenomen. Schietsportvereniging Veldhoven weegt hier de belangen en rechten van de leden en bezoekers af tegen zijn eigen belang.

DPIA
In dit document is een DPIA opgenomen om de juiste afwegingen te maken.

Rechten leden en bezoekers
Schietsportvereniging Veldhoven zorgt ervoor dat de leden en bezoekers weten dat er een camera hangt en voor welk doel deze er hangt. Bijvoorbeeld door bordjes op te hangen.

Daarnaast geeft de Algemene verordening gegevensbescherming (AVG) de volgende privacy rechten aan betrokkenen:

- het recht om gegevens (camerabeelden) in te zien;
- het recht om vergeten te worden;
- het recht op beperking van de verwerking;
- het recht om bezwaar te maken tegen het gebruik van persoonsgegevens.

Bewaartermijn camerabeelden
Schietsportvereniging Veldhoven bewaart de camerabeelden niet langer dan noodzakelijk. De richtlijn hiervoor is maximaal 4 weken.
Maar is er een incident vastgelegd, zoals diefstal? Dan mag Schietsportvereniging Veldhoven de betreffende beelden bewaren tot dit incident is afgehandeld.

Voor welke soorten verwerkingen is het uitvoeren van een DPIA verplicht?
De autoriteit Persoonsgegevens (AP) heeft een lijst van verwerkingen opgesteld waarvoor het uitvoeren van een data protect impact assessment (DPIA) altijd verplicht is voor u met verwerken begint.

Uw verwerking moet altijd voldoen aan de Algemene verordening gegevensbescherming (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 afgestemd in EU-verband. Periodiek bekijken de EU-privacy toezichthouders of de lijst moet worden aangepast.

In deze lijst staat het volgende vermeldt over Camerasystemen.

Cameratoezicht
Grootschalige verwerkingen en/of stelselmatige monitoring van openbaar toegankelijke ruimten met camera's, webcams of drones.
Dit houdt in dat we een DPIA moeten opstellen voor dit project.

Wie moet een DPIA uitvoeren?
Als verantwoordelijke moet u ervoor zorgen dat er een data protection impact assessment (DPIA) wordt uitgevoerd. U moet hierbij, wanneer van toepassing, aan verschillende partijen advies vragen. U hoeft de DPIA niet zelf uit te voeren, dit kunt u ook door iemand anders binnen of buiten uw organisatie laten doen. U blijft wel eindverantwoordelijk.

Gerechtvaardigd belang
Allereerst wordt er gekeken naar een gerechtvaardigd belang

Voorwaarden grondslag gerechtvaardigd belang
De 3 voorwaarden zijn:

1. U heeft daadwerkelijk een gerechtvaardigd belang. Niet elk belang kwalificeert als een gerechtvaardigd belang.
2. De verwerking is noodzakelijk om dit belang te behartigen.
3. U heeft een afweging gemaakt tussen uw belangen en die van de betrokkenen.

Voorwaarde 1: gerechtvaardigd belang
Uw belang is daadwerkelijk een gerechtvaardigd belang als het ergens in het recht is opgenomen. En wordt erkend en beschermd. Dat mag ook in een ongeschreven rechtsregel of rechtsbeginsel zijn.

Schietsportvereniging Veldhoven gebruikt het Video Surveillance Systeem niet met commercieel belang of winst verruiming. Het Video Surveillance Systeem wordt niet gebruikt om het gedrag van leden en bezoekers te volgen zonder legitieme redenen. Het is tevens niet om het gedrag van bezoekers te volgen zonder legitieme redenen.

Het Video Surveillance Systeem is alleen werkzaam op en rondom de schietbaan. Omdat hier met dodelijke wapens geschoten wordt kan er alleen op deze manier toezicht gehouden worden op de schietbaan. Dit is om het veiligheidsgevoel van leden en bezoekers te vergroten en op de schietbaan toezicht te houden om mogelijke incidenten en calamiteiten te signaleren en hierop te handelen.

Voorwaarde 2: noodzakelijkheid
Heeft u daadwerkelijk een gerechtvaardigd belang? Dan moet u vervolgens kijken of de verwerking van persoonsgegevens noodzakelijk is om dit belang te behartigen. Dit doet u door na te gaan:

Of het doel van uw verwerking in verhouding staat tot de inbreuk op de privacy van de betrokkenen. In de AVG heet dit ‘proportionaliteit’.
Of u het doel niet op een andere manier kunt bereiken, die minder ingrijpend is voor de betrokkenen. In de AVG heet dit ‘subsidiariteit’.

Schietsportvereniging Veldhoven is van mening dat dit niet op een andere manier op te lossen is. Het is niet mogelijk om op de schietbaan personen neer te zetten om alle handelingen van de schutters te monitoren.
De inbreuk op de privacy van de leden en bezoekers wordt geminimaliseerd tot alleen de schietbaan.

Tevens houdt Schietsportvereniging Veldhoven er rekening mee dat de beelden maximaal 4 weken wordt bewaard.

De doelstellingen zijn duidelijk omschreven en worden aan alle leden en bezoekers duidelijk gemaakt door interne communicatie en borden rondom het terrein zodat iedereen op de hoogte is dat er 24/7 Video Surveillance plaats vindt op het terrein.

Schietsportvereniging Veldhoven heeft de regel dat er maar een beperkt aantal personen de mogelijkheid krijgen om de beelden terug te kijken of de beelden te bekijken.
Hierbij hanteert de vereniging altijd het 4 ogen principe.

In de recorder wordt altijd gelogd wie er ingelogd is op welke tijd. Dus dit is te achterhalen. Verder wordt ervoor gezorgd dat bij geen werkzaamheden op het Video Surveillance Systeem de gebruiker automatisch wordt uitgelogd. De gebruikers kunnen zelf niets opslaan op hun eigen computer. Dit dient ten alle tijden te gebeuren in de serverruimte.

Tevens zijn alle beelden en dataverkeer ge-encrypt.

Voorwaarde 3: afweging belangen
Heeft u een gerechtvaardigd belang en is de gegevensverwerking noodzakelijk om dit belang te behartigen? Dan moet u tot slot een afweging maken tussen uw belangen en de belangen van de betrokkenen.
Bij deze afweging kijkt u naar:

- de gevolgen voor de betrokkenen;
- hoe ernstig de inbreuk is op de privacy van de betrokkenen;
- welke (aanvullende) maatregelen u heeft genomen om ongewenste gevolgen voor de betrokkenen te voorkomen of beperken;
- of de betrokkenen de verwerking min of meer kunnen verwachten, bijvoorbeeld als vervolg op een eerdere verwerking waarvoor zij toestemming hebben gegeven of als vervolg op verwerkingen die noodzakelijk zijn om een contract uit te voeren.

De gevolgen en de inbreuk op de privacy van de leden en bezoekers wordt tot een minimum beperkt doordat er alleen beelden teruggekeken wordt als dit strikt noodzakelijk is.
Het aantal mensen dat de beelden kan bekijken wordt beperkt tot minimaal.
De beelden worden automatisch overschreven na maximaal 4 weken.

Er wordt bijgehouden door Schietsportvereniging Veldhoven wie er wanneer beelden heeft bekeken en wat daar de reden van is. Iedere gebruiker heeft eigen login gegevens en wordt gelogd. Er is een automatische uitlog geprogrammeerd zodat bij een bepaalde tijd het systeem automatisch wordt uitgelogd.

Conclusie Gerechtvaardigd belang
Schietsportvereniging Veldhoven komt hierdoor tot de conclusie dat er een gerechtvaardigd belang is om het Video Surveillance Systeem in te zetten en dat er voldoende maatregelen getroffen worden om de inbreuk op de privacy van leden en bezoekers tot een minimum te beperken.

Het Video Surveillance Systeem wordt alleen gebruikt voor:

- Eigendommen van het bedrijf te beschermen
- Iemand aansprakelijk kunnen stellen voor schade
- Computersystemen en andere systemen te beveiligen en te beschermen
- Om aan alle verplichtingen te voldoen die het bedrijf en de personen hebben op basis van de wetten geldend in Nederland
- Het beschermen van leden aangezien er geschoten wordt met wapens
- Het in beeld brengen van handelingen op de schietbaan die gevaarlijk kunnen zijn en de veiligheid in het geding kunnen brengen

Wat zijn de criteria van de Europese Privacy toezichthouders?
De Europese privacy toezichthouders hebben 9 criteria opgesteld om te beoordelen of uw voorgenomen verwerking van persoonsgegevens een hoog privacy risico 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.

Conclusie: Schietsportvereniging Veldhoven beoordeeld met het Video Surveillance systeem mensen niet op basis van Persoonskenmerken.

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 guidelines over geautomatiseerde besluitvorming en profilering van de Europese privacy toezichthouders.

Conclusie: Schietsportvereniging Veldhoven gebruikt het Video Surveillance systeem niet om met automatische beslissingen mensen uit te sluiten of te discrimineren.

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.

Conclusie: Door middel van borden en stickers wordt aangegeven dat er een Video Surveillance systeem aanwezig is. In dit document wordt duidelijk omschreven waarom er gegevensverwerking plaats vindt. De beelden worden alleen teruggekeken op basis van incidenten en calamiteiten door het bestuur van de vereniging. Andere leden hebben ook geen toegang tot het terugkijken van beelden.

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.

Conclusie: Het Video Surveillance Systeem wordt hier niet voor gebruikt.

5. Grootschalige gegevensverwerkingen
De AVG geeft geen definitie van ‘grootschalige gegevensverwerkingen’. De Europese privacy toezichthouders 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.
Zie ook: wat ziet de AVG als een grootschalige verwerking van persoonsgegevens?

Conclusie: Het Video Surveillance systeem wordt hier niet voor gebruikt.

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.

Conclusie: Het Video Surveillance Systeem is een systeem wat stand-alone draait en niet gekoppeld wordt aan andere systemen die gegevens verzamelen of gebruik maakt van databases.

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 leden en bezoekers gaan.

Conclusie: Het Video Surveillance Systeem wordt hier niet voor gebruikt.

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 privacy risico’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.

Conclusie: Omdat het gaat om een Video Surveillance Systeem is er in dit document een DPIA opgenomen om de afwegingen die gemaakt zijn uit te leggen en inzichtelijk te maken.

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.

Conclusie: Het Video Surveillance Systeem wordt hier niet voor gebruikt.

DPIA - data protection impact assessment
Er is tot de conclusie gekomen dat er een gerechtvaardigd belang is. Nu is het noodzaak om te kijken door middel van een DPIA wat de impact verder is op de privacy

Beschrijving van de beoogde gegevensverwerkingen en de doeleinden hiervan
Bij Schietsportvereniging Veldhoven is er een Video Surveillance Systeem aanwezig.
Om goed toezicht te houden op de schietbaan zijn er camera's aanwezig die de verschillende schietbanen in beeld brengen. Dit is nodig om het handelen van de schutters in beeld te brengen en toezicht te kunnen houden op de schietbaan. Dit zal de veiligheid op de schietbaan ten goede brengen.

Doelstellingen van het Video Surveillance Systeem
Het Video Surveillance Systeem heeft als doel:

1. Het verhogen van het veiligheidsgevoel van de leden
2. Preventieve werking tegen ongewenste activiteiten
3. Toezicht op de schietbaan
4. Ondersteunend bij reconstructie van ongewenste gebeurtenissen

De camera's zijn zo geprojecteerd en kunnen gebruikt worden voor waarneming, herkenning en/of identificatie van personen en/of gebeurtenissen

Voorbeelden van: waarnemen, herkennen en identificeren

De camera's zijn geprojecteerd als waarnemen en identificeren

Er wordt een recorder geplaatst. Tot deze recorder hebben alleen de noodzakelijke personen toegang.

Bewaartermijn camerabeelden
Schietsportvereniging Veldhoven bewaart de camerabeelden niet langer dan noodzakelijk. De richtlijn hiervoor is maximaal 4 weken. Na 4 weken worden de beelden automatisch overschreven.

Maar is er een incident vastgelegd, zoals diefstal? Dan bewaard Schietsportvereniging Veldhoven de betreffende beelden tot dit incident is afgehandeld.

Bekijken en terugkijken van camerabeelden
De beelden worden op verschillende plaatsen Live bekeken. Deze personen hebben ook geen rechten om beelden terug te kijken.
Het recht tot terugkijken van de beelden is binnen Schietsportvereniging Veldhoven beperkt tot personen die zijn aangesteld door de organisatie.

Aanduiding op en rondom het terrein
Er wordt aangeduid dat er een videosurveillance systeem aanwezig is.

Rechten leden en bezoekers
Mensen hebben verschillende rechten om controle te houden over hun persoonsgegevens. In dit dossier vindt u praktische informatie en tips voor organisaties over het omgaan met privacy rechten in de praktijk.

Gezond privacy beleid
Gehoor geven aan mensen die een beroep doen op hun privacy rechten is een belangrijk onderdeel van een gezond privacy beleid. En een gezond privacy beleid draagt bij aan het vertrouwen van mensen in uw organisatie.

Zorg er daarom voor dat u uw systemen, processen en interne organisatie inricht op deze rechten. Zodat u op de juiste manier gehoor kunt geven aan verzoeken van betrokkenen.

De AVG-privacy rechten
Recht op inzage. Dat is het recht van mensen om onder meer een kopie te ontvangen van de persoonsgegevens die u van hen verwerkt. De Autoriteit Persoonsgegevens (AP) biedt u een voorbeeldoverzicht.
Recht op vergetelheid. Mensen hebben het recht om ‘vergeten’ te worden. Maar wist u dat u vaak niet alle persoonsgegevens kunt wissen?
Recht op rectificatie en aanvulling. Het recht om de persoonsgegevens die u verwerkt te laten wijzigen.

Het recht op data-portabiliteit. Het recht om persoonsgegevens over te laten dragen aan een andere partij.

Het recht op beperking van de verwerking: Het recht om minder gegevens te laten verwerken.

Het recht met betrekking tot geautomatiseerde besluitvorming en profilering. Oftewel: het recht op een menselijke blik bij besluiten.

Het recht om bezwaar te maken tegen de gegevensverwerking.

Ten slotte hebben mensen recht op duidelijke informatie over wat u met hun persoonsgegevens doet. Onder de AVG moet u aan een aantal specifieke eisen voldoen.

Identiteit vaststellen
Wanneer iemand zijn/haar privacy rechten bij u uitoefent, moet u checken of die persoon is wie hij of zij zegt te zijn. U wilt immers voorkomen dat u iemand toegang geeft tot de persoonsgegevens van een ander.

U mag voor dit doel bijna nooit een volledige kopie van het identiteitsbewijs vragen. In de meeste gevallen zijn er namelijk minder ingrijpende manieren om iemands identiteit vast te stellen.

Maar mocht het in uw geval wél passend zijn om een kopie van iemands ID te vragen, let er dan op dat u bepaalde informatie moet geven aan deze persoon.

Register van verwerkingen opstellen
U moet een register van verwerkingsactiviteiten opstellen.
U heeft aangegeven dat uw situatie voldoet aan één van de criteria voor het opstellen van een register van verwerkingsactiviteiten. Als dat klopt dan bent u volgens de AVG verplicht om een register van verwerkingsactiviteiten op te stellen.

Actiepunt:
Stel een register van verwerkingsactiviteiten op. Op autoriteitpersoonsgegevens.nl leest u wat er in zo'n register moet staan.

Wat moet er in een Register van Verwerkingen staan?
Het register van verwerkingsactiviteiten (verwerkingsregister) bevat informatie over de persoonsgegevens die u verwerkt. U mag zelf weten hoe u het register opstelt. Wel schrijft de Algemene verordening gegevensbescherming (AVG) voor welke informatie u als verantwoordelijke of verwerker in het verwerkingsregister moet zetten.

Verplicht verwerkingsregister
U bent onder de AVG vrijwel altijd verplicht om een register van verwerkingsactiviteiten (verwerkingsregister) bij te houden.

Is uw organisatie de verwerkingsverantwoordelijke?
Stelt uw organisatie zelf het doel en de middelen voor de verwerking van de persoonsgegevens vast? Dan is uw organisatie de verwerkingsverantwoordelijke.

De AVG schrijft voor dat u als verwerkingsverantwoordelijke de volgende informatie in het register moet opnemen:

Naam en contactgegevens
De naam en contactgegevens van:
- uw organisatie of de vertegenwoordiger van uw organisatie;
- eventuele andere organisaties met wie u gezamenlijk de doelen en middelen van de verwerking heeft vastgesteld;
- de functionaris gegevensbescherming (FG), als u die heeft aangesteld; (indien nodig)
- eventuele internationale organisaties waar u persoonsgegevens mee deelt.

Doeleinden
De doelen waarvoor u de persoonsgegevens verwerkt. Bijvoorbeeld voor de werving en selectie van personeel, het bezorgen van producten of direct marketing.

Tip: het is aan te raden om hierbij ook de grondslag te vermelden voor elk van uw verwerkingen. U bent dit niet verplicht volgens de AVG, maar het kan wel helpen om aan uw verantwoordingsplicht te voldoen.
Deze staan in dit document vermeldt.

Betrokkenen
Een beschrijving van de categorieën van personen van wie u gegevens verwerkt. Bijvoorbeeld uitkeringsgerechtigden, klanten of patiënten.

Persoonsgegevens
Een beschrijving van de categorieën van persoonsgegevens. Zoals het BSN, NAW-gegevens, telefoonnummers, camerabeelden of IP-adressen.
In dit geval bestaat dit uit camerabeelden

Bewaartermijn
De datum waarop u de gegevens moet wissen (als dat bekend is).
Bewaartermijn is in de DPIA opgenomen

Ontvangers
De categorieën van ontvangers aan wie u persoonsgegevens verstrekt.
De informatie blijft intern

Buiten EU
Deelt u de gegevens met een land of internationale organisatie buiten de EU? Dan moet u dit aangeven in het verwerkingsregister.

Beveiliging
Een algemene beschrijving van de technische en organisatorische maatregelen die u heeft genomen om de persoonsgegevens die u verwerkt te beveiligen.

Is uw organisatie een verwerker?
Verwerkt u in opdracht van een verantwoordelijke persoonsgegevens? Bijvoorbeeld omdat u werkt bij een administratiekantoor of een onlinedienst voor gegevensopslag? Dan moet de volgende informatie in uw verwerkingsregister staan:

Naam en contactgegevens
De naam en contactgegevens van:
- uw organisatie, of de vertegenwoordiger van uw organisatie, of de verwerkingsverantwoordelijke;
- de functionaris gegevensbescherming (FG), als u die heeft aangesteld.

Verwerkingen
- Een beschrijving van de categorieën van verwerkingen die u in opdracht van iedere verantwoordelijke uitvoert.

Internationale doorgifte
Eventuele internationale organisaties waarmee u persoonsgegevens deelt.

Buiten EU
Deelt u de gegevens met een land of internationale organisatie buiten de EU? Dan moet u dit aangeven in het verwerkingsregister.

Beveiliging
Een algemene beschrijving van de technische en organisatorische maatregelen die u heeft genomen om de persoonsgegevens die u verwerkt te beveiligen.

Privacy beleid
U bent alleen verplicht om een privacy beleid (gegevensbeschermingsbeleid) op te stellen als dat in verhouding staat tot uw verwerkingsactiviteiten. Of u verplicht bent om een privacy beleid op te stellen, hangt af van de concrete omstandigheden. Zoals de aard, de omvang, de context en het doel van de gegevensverwerking.

Ziekenhuizen, gemeenten, socialmedia-bedrijven en handelsinformatiebureaus zullen daarom vaak verplicht zijn om een privacy beleid op te stellen. Ook kleine organisaties kunnen verplicht zijn een privacy beleid op te stellen.

Vrijwillig privacy beleid
Bent u niet verplicht om een privacy beleid op te stellen? Dan kan het toch nuttig zijn om dat wél te doen.

Het helpt u namelijk om te zien of u voldoende maatregelen heeft genomen om de persoonsgegevens van bijvoorbeeld uw klanten, patiënten of cliënten te beschermen.

Daarnaast is het een manier waarmee u aan zowel uw doelgroep als de Autoriteit Persoonsgegevens kunt laten zien dat u voldoet aan de Algemene verordening gegevensbescherming (AVG).

Verschil met privacyverklaring
Let op: een privacy beleid is iets anders dan een privacyverklaring. Niet elke organisatie die persoonsgegevens verwerkt, is verplicht een privacy beleid op te stellen.

Maar iedere organisatie is wél verplicht om mensen heldere informatie te geven over de persoonsgegevens die de organisatie verwerkt en voor welke doelen dat gebeurt.

In de praktijk is een online privacyverklaring de handigste manier om aan deze verplichting te voldoen.

Wat moet er volgens de AVG in een privacy beleid staan?

In de Algemene verordening gegevensbescherming (AVG) staat niet precies omschreven welke gegevens u in uw privacy beleid (gegevensbeschermingsbeleid) moet opnemen. Uit het beleid moet in ieder geval blijken hoe u voldoet aan de AVG.

Dat is onderdeel van uw verantwoordingsplicht.

Informatie in privacy beleid
U kunt laten zien hoe u voldoet aan de AVG door onder andere deze informatie op te nemen:

Een omschrijving van de categorieën persoonsgegevens die u verwerkt.
Een beschrijving van de doeleinden waarvoor u persoonsgegevens verwerkt. En wat de wettelijke grondslag daarvoor is.
Hoe u voldoet aan de beginselen van verwerking van persoonsgegevens. Zoals de verplichting om niet meer gegevens te verwerken dan noodzakelijk.

- Welke privacy rechten betrokkenen hebben en hoe zij die rechten kunnen uitoefenen. Zoals het recht om een klacht in te dienen bij de Autoriteit Persoonsgegevens (AP). Maar ook het recht op inzage, wijzigen, wissen en het ontvangen van alle geregistreerde gegevens.
- Welke organisatorische en technische maatregelen u genomen heeft om de persoonsgegevens te beveiligen.
- Hoe lang u de persoonsgegevens bewaart.

Het opstellen van een privacy beleid is niet altijd verplicht. Toch kan het nuttig zijn om ook een privacy beleid op te stellen als u dit niet verplicht bent.

Deze gegevens staan allemaal verwerkt in dit document

Checklist: Houd grip op persoonsgegevens
Privacybescherming is een continu proces. En draagt bij aan het vertrouwen van mensen in uw organisatie. Deze checklist helpt u om te toetsen of uw organisatie (nog steeds) aan een aantal belangrijke AVG-verplichtingen voldoet. Zodat u weet of, en zo ja waar, u in actie moet komen.

1. Heeft u zicht op alle verwerkingen?
Het type gegevens dat uw organisatie verwerkt heeft gevolgen voor de manier waarop u die moet beschermen. En aan welke AVG-regels u zich moet houden.

Ter illustratie: ga bijvoorbeeld na of u niet per ongeluk bijzondere persoonsgegevens verwerkt. Want dat is in de meeste gevallen verboden.

2. Heeft u nog steeds een grondslag?
U mag alleen persoonsgegevens verwerken wanneer u daarvoor een grondslag heeft. Ga daarom na of dat voor al uw verwerkingen zo is.

Ter illustratie: is een verwerking niet langer 'noodzakelijk voor de uitvoering van een overeenkomst'? Dan mag u zich niet meer op die grondslag baseren.

3. Zijn uw (nieuwe) medewerkers privacybewust?
Zijn bestaande en nieuwe medewerkers goed op de hoogte van de privacyregels? Zij spelen immers een belangrijke rol in het privacyproof houden van uw processen, diensten en producten.

Tip: overweeg of het nodig is om (bepaalde) AVG-regels extra onder de aandacht te brengen.

4. Kunnen mensen hun privacyrechten uitoefenen?
Ga na of uw organisatie de afgelopen tijd verzoeken heeft ontvangen van mensen die hun privacyrechten willen uitoefenen. En of die snel en volgens de regels zijn afgehandeld. Zijn uw processen op orde?

Ga ook na of uw organisatie zich aan de eigen bewaartermijnen houdt. Verwijder gegevens die u niet langer nodig heeft.

5. Is uw overzicht met verwerkingen nog up to date?
Vaak bent u onder de AVG verplicht om een verwerkingsregister bij te houden. Ga in dat geval na of alle (nieuwe) verwerkingen in het verwerkingsregister staan.

Het bijhouden van een overzicht van verwerkingen is onderdeel van uw verantwoordingsplicht.

6. Moet u een DPIA uitvoeren?

In sommige gevallen kunt u verplicht zijn om een data protection impact assessment (DPIA) uit te voeren voordat u mag starten met de verwerking. Ga na of u dat in de juiste gevallen ook heeft gedaan. En of het nodig is voor eventuele nieuwe verwerkingen waarmee u wilt starten.

Heeft u al eens een DPIA uitgevoerd? En aan de hand daarvan maatregelen genomen om bepaalde privacyrisico's te verkleinen? Ga dan na of die maatregelen nog steeds voldoende zijn.

7. Werkt u volgens privacy by design en default?

Past uw organisatie de verplichte uitgangspunten van privacy by design en privacy by default goed toe in de praktijk?

Bijvoorbeeld omdat:
- een app die u aanbiedt niet de locatie van gebruikers registreert als dat niet nodig is;
- op uw website het vakje 'Ja, ik wil aanbiedingen ontvangen' niet vooraf staat aangevinkt;
- als iemand zich op uw nieuwsbrief wil abonneren u niet meer gegevens vraagt dan nodig is.

8. Heeft u een FG of privacycontactpersoon?

Ga na of uw organisatie verplicht is om een functionaris gegevensbescherming (FG) aan te stellen. Zeker wanneer de omvang en activiteiten van uw organisatie zijn veranderd.

Komt u tot de conclusie dat een FG voor u niet verplicht is? Overweeg dan of het kan helpen om vrijwillig een privacycontactpersoon aan te stellen.

9. Kunt u snel handelen bij datalekken?

Check of u bent voorbereid op een datalek. Hebben zich de afgelopen tijd bijvoorbeeld beveiligingsincidenten in uw organisatie voorgedaan? Zo ja, zijn de processen in uw organisatie zo ingericht dat er snel is gehandeld? Zijn datalekken tijdig bij de AP gemeld? En zijn ze goed gedocumenteerd?

10. Heeft u grip op uw verwerkers?

Heeft u uw gegevensverwerking uitbesteed aan een verwerker? Beoordeel dan of de overeengekomen maatregelen in bestaande contracten met uw verwerkers nog steeds toereikend zijn. En in de praktijk worden nageleefd.