

AVG verkenning VSA

Inhoud

AVG verkenning VSA	1
Inleiding.....	2
Aanleiding en doel.....	2
Methode	2
Samenvatting.....	3
Algemene afdronk	3
Samenvatting per bureau en VSA breed.....	3

Inleiding

Aanleiding en doel

Sinds 25 mei 2018 is de Algemene verordening gegevensbescherming (AVG) van toepassing. De AVG schrijft voor hoe organisaties om moeten gaan met het verzamelen, verwerken, opslaan en verwijderen van persoonsgevoelige informatie.

De volgende regels moeten worden gevolgd:

- transparantie: de persoon van wie de gegevens verwerkt worden, is hiervan op de hoogte, heeft hiervoor toestemming gegeven en kent zijn rechten.
- doelbeperking: de persoonsgegevens worden voor een welbepaald gewettigd doel verzameld, en mogen niet voor andere zaken gebruikt worden.
- gegevensbeperking: enkel de gegevens die voor het beoogde doel noodzakelijk zijn, mogen worden verzameld.
- juistheid: de persoonsgegevens moeten correct zijn en blijven.
- bewaarbeperking: de persoonsgegevens mogen niet langer bewaard worden dan nodig voor het beoogde doel.
- integriteit en vertrouwelijkheid: de persoonsgegevens moeten beschermd worden tegen toegang door onbevoegden, verlies of vernietiging.
- verantwoording: de verantwoordelijke moet kunnen aantonen aan deze regels te voldoen.

De afdeling VSA gebruikt allerlei persoonsgegevens. Van gegevens nodig voor aan- en verkoop van panden, tot gegevens uit vragenlijsten, boekingen etc. De afgelopen jaren is er steeds meer aandacht voor de vertrouwelijkheid van informatie bij VSA en de maatregelen die nodig zijn om veilig te handelen. Er wordt steekproefsgewijs gekeken hoe de verschillende bureaus ermee omgaan, maar een volledig overzicht van welke gevoelige informatie de afdeling precies heeft en hoe er mee om wordt gegaan, ontbreekt. Daarom was gevraagd om een verkennend onderzoek, om dit voor de afdeling in beeld te brengen.

Doel

Met dit onderzoek willen we verder *in control* komen op het gebied van AVG op de afdeling: we willen weten bij welke processen en/of organisatieonderdelen er binnen VSA gebruik gemaakt wordt van verschillende persoonsgevoelige gegevens, hoe daar mee om wordt gegaan, wat onzekerheden en risico's zijn en hoe we met deze risico's om moeten of willen gaan (risicobereidheid). Om zo meer inzicht en grip te krijgen op de AVG bij VSA en te kunnen bepalen welke vervolgstappen er nodig zijn om de afdeling verder AVG-proof te krijgen. Hierbij is gekeken naar gebruikte systemen, processen en gegevens (op hoofdlijnen) en naar welk gedrag en bewustzijn daarvoor nodig is onder medewerkers.

Daarnaast draagt dit onderzoek bij aan de jaarlijkse verantwoording van VSA aan de Functionaris Gegevensbescherming (FG). De afgelopen jaren is de rol van de Functionaris Gegevensbescherming (FG) en de Privacy Officer (PO) steeds meer vormgegeven in de organisatie. Zij hebben een controlerende (FG) en adviserende (PO) rol wat betreft de waarborging van de vertrouwelijkheid van persoonsgegevens. De FG moet uiteindelijk kunnen verantwoorden aan de Autoriteit Persoonsgegevens.

Methode

De informatie is opgehaald via gesprekken met leidinggevendenden, omdat zij een overzicht van hun bureau hebben. Waar relevant zijn verdiepende gesprekken met andere medewerkers gevoerd. De constatering in dit stuk zijn voornamelijk op basis van indrukken en uitleg van de leidinggevendenden en overige medewerkers. Omdat dit onderzoek ging om een verkenning op de afdeling, is niet tot in detail in systemen en correspondentie gekeken of steekproefsgewijs getoetst.

De gesprekken zijn uitgewerkt in notulen, zodat preciezer na te lezen is wat met deelnemers besproken is. De informatie is vervolgens, voor het overzicht, samengevat.

Samenvatting

Algemene afdronk

De afdeling maakt op meerdere plekken gebruik van persoonsgegevens. Zoals bij contact met huurders (assetmanagers), het afsluiten van abonnementen (recreatie) en contact met inwoners die graag willen sporten. Aan het verwerken van gegevens zitten grofweg twee elementen. Ten eerste het inregelen van veilige systemen, autorisaties en de afspraken daarom heen. Ten tweede het gedrag van medewerkers: wordt er aan afspraken gehouden, zijn medewerkers zich bewust van AVG en hun rol daarin?

Voor zowel het inregelen van veilige systemen als voor gedrag is de indruk dat er rekening gehouden wordt met AVG en dat de afgelopen jaren de nodige maatregelen zijn getroffen. Daarmee lijkt VSA aardig op weg te zijn en in zekere mate *in control* te zijn. Wel is er een aantal maatregelen dat genomen kan/moet worden en blijft het nodig om in de bureaus af en toe stil te staan bij AVG. Een datalek of onjuist gebruik van persoonsgegevens zit in een klein hoekje. Daarnaast blijft het altijd zoeken naar de balans tussen risico's volledig afdekken (bv. slechts een of twee personen ergens toegang toe geven) en het werkbaar houden (bv. elkaar kunnen vervangen bij uitval).

Er is in de gesprekken specifiek gevraagd naar voorvallen en klachten met AVG de afgelopen jaren. Deze zijn weinig genoemd. Het is daarmee geen bewijs dat alles goed geregeld is, maar het ondersteunt de indrukken uit gesprekken: dat in veel processen, systemen en werkzaamheden wel rekening gehouden wordt met AVG. Het is belangrijk om te beseffen dat het hier om een momentopname gaat. Dit onderzoek heeft een periodieke update nodig. De FG geeft aan twee toets momenten per jaar te hebben.

Samenvatting per bureau en VSA breed

Vastgoed	
Globale stand van zaken	<p>Vastgoed kent 3 basisprocessen verhuurproces, bouwproces en verkoopproces, verdeeld over de deelbureaus portefeuillemanagement, assetmanagement en het bouwteam. Daarnaast zijn archivering en het contact met Heyday van belang.</p> <p>Bouwteam Het bouwteam en het bouwproces hebben weinig te maken met AVG. In de basis werken zij samen met zakelijke contacten. Contact met eventuele huurders loopt via de assetmanager.</p> <p>Uitzonderingen: contact met een privénummer, bijvoorbeeld met een voorzitter van een vereniging (zelden), in mailcontact met externen kan een privéadres voorbijkomen (niet structureel) of er wordt een privé-emailadres gegeven om notulen naartoe te sturen. Hierbij wordt dan niet altijd expliciet om toestemming gevraagd.</p> <p>Assetmanagement Bij assetmanagement zijn contracten en correspondentie belangrijk. Een tijdje terug is door een aantal collega's een project gestart voor het AVG-proof maken van huurcontracten. In de standaard huurcontracten en (opstal)overeenkomsten zijn nu artikel 14 (informatieverstrekking derden) en 15 (recht van inzage) verwerkt. In eerdere jaren vroegen assetmanagers om kopieën van paspoorten. Dat mag niet (meer). De indruk van gesproken collega's is dat er nu redelijk AVG-proof gewerkt wordt.</p> <p>Planon. We hebben contactgegevens van personen waarbij in het pand aan onderhoud gedaan moet worden. Dit gaat bijvoorbeeld over woningen en standplaatsen. Met deze personen is een (huur)contract afgesloten, deze worden opgeslagen in Planon. Op dit moment kunnen veel mensen die in Planon werken dit inzien. Hoe doe je dit handig? Je wilt ook werk kunnen overnemen als iemand ziek is bijvoorbeeld. Planon bestaat uit meerdere modules, per module kan een gebruikersgroep toegang krijgen. In mailcontact met privépersonen is geen standaardzin verwerkt over persoonsgegevens. In Planon staan ook</p>

	<p>WOZ-waardes, vanuit een interfase vanuit het belastingsysteem. Hierin zijn geen persoonsgegevens meer te zien.</p> <p>Bij het vastgoedloket komen vragen die inwoners hebben over een pand, of een klacht die ze melden. Het initiatief komt hierbij vanuit de bewoner. De vraag of klacht komt binnen via een website waarbij je met DigID inlogt. Hiermee worden gegevens op een veilige manier verwerkt.</p> <p>Portefeuillemanagement Bij PM is weinig sprake van persoonsgegevens. Het gaat vaak om maatschappelijk vastgoed. Panden waar inwoners in wonen worden vaak op pandniveau besproken, hier komen geen persoonsgegevens aan te pas.</p> <p>Archivering Er is afgesproken dat als zaken te maken hebben met een huurder, er dan een los dossier wordt aangemaakt. De huurder moet 2 jaar later uit het systeem (verplichte bewaartermijn). Bij het archiveren wordt deze termijn handmatig aangegeven. Daarna ligt de verantwoordelijkheid bij BDI. BDI krijgt een automatisch signaal na de bewaartijd. Zij sturen dan een lijst met informatie op naar Vastgoed, om te checken of de gegevens inderdaad verwijderd kunnen worden. Daarnaast zijn er ook nog 'ruimtevragen', bijvoorbeeld omdat iemand een yoga-ruimte zoekt. Deze worden op één plek verzameld, na een jaar wordt dit verwijderd.</p> <p>Heyday Er zijn algemene afspraken met Heyday over het gebruik van gegevens, namelijk dat gegevens alleen gebruikt worden als dat noodzakelijk is, bijvoorbeeld bij een verbouwing. Er ligt nog geen verwerkingsovereenkomst hieronder. De indruk van de contractmanager is dat Heyday serieus omgaat met de afspraken en zorgvuldig met gegevens omgaat. Een tijdje geleden is nog tussen de contractmanager en Heyday gesproken over de geheimhoudingsverklaring. In contracten met onderaannemers hebben zij ook een vermelding hierover. Er is niet specifiek over AVG gesproken. Heyday maakt gebruik van 'Facilitor'. Daarin staan panden met persoonsgegevens. Assetmanagers kunnen dit inzien. Heyday heeft een verwerkingsovereenkomst met Facilitor over het gebruik van (persoons)gegevens.</p>
Systemen totaal	<ul style="list-style-type: none"> - Planon (+ gebouwenpaspoort) - Atlaz - Tableau: dashboard met managementinfo (in ontwikkeling) - Facilitor (Heyday) - Outlook - Word - CODA - Excel - iPhone - G-schijf & Gemeenschappelijke schijf
Belangrijkste risico's	<ul style="list-style-type: none"> - Assetmanagement heeft het meeste contact met privépersonen. Hierbij is bewustzijn over gevoelige informatie en het vragen om toestemming van gebruik gegevens belangrijk. - In stand houden: er wordt veel gebruik gemaakt van standaard formats. Afspraak is dat er lege formats gebruikt worden, zodat niet per ongeluk gegevens overgenomen worden. - In Planon en de gebouwenpaspoorten staan persoonsgegevens. Af en toe is een update nodig: wie heeft rechten/toegang hiertoe en is dit nog steeds terecht? Daarnaast blijft het belangrijk om vertrouwelijk met de autorisaties om te gaan.
Mogelijke acties	<ul style="list-style-type: none"> - AVG weer op frissen in de teams. Wat mag wel, wat mag niet? Waar loopt men tegenaan, wat zijn nog vragen? Kloppen alle autorisaties nog? - Opstellen verwerkingsovereenkomst met Heyday. - DPIA maken voor Planon (incl. gebouwenpaspoort), in samenwerking met Facilitaire zaken.

Sport

Globale stand van zaken

Sport is opgedeeld in sportontwikkeling, binnensport- en buitensportaccommodaties.

Sportontwikkeling

Sportontwikkeling kent drie functies: buurtsportcoaches, sportdocenten en sportconsultanten.

Buurtsportcoaches hebben veel 'losse' contacten met bewoners (beweeg-adviesgesprekken). Dit komt vanuit een doorverwijzing of ze verwijzen zelf door. Hierin worden dus veel persoonsgegevens gedeeld. De indruk van de gesproken leidinggevende is dat BSC-ers redelijk bewust zijn van hoe ze met persoonsgegevens om moeten gaan en altijd om toestemming vragen voor het doorsturen van gegevens.

Elk team houdt bij hoeveel beweegadviesgesprekken zij houden. Dit doen ze zonder dat de informatie te herleiden is naar personen.

De buurtsportcoaches halen ook bij scholen op wat de sportparticipatie van leerlingen is. Hierbij worden slechts aantallen genoemd, geen personen. De school is dus de tussenpartner. De uitdaging hierbij is vooral dit van tevoren goed in te regelen met scholen. Zijn er eenmaal heldere afspraken, dan loopt het vaak wel.

De buurtsportcoaches organiseren ook projecten en evenementen. Vaak met een aanmeldsysteem (bijvoorbeeld via een QR-code), waarbij je toestemming moet geven voor het gebruik van persoonsgegevens.

Vaak wordt er ook met WhatsApp-groepen gewerkt. De leidinggevende is er niet zeker van of hier altijd goed om toestemming gevraagd wordt.

Sportdocenten organiseren veel sportevenementen en projecten in de wijk. Daar komen ook vaak WhatsApp groepen bij kijken. Ook hiervoor weet de leidinggevende niet precies of deze toestemming altijd gevraagd wordt. Daarnaast zijn er sportgroepen voor ouderen, waar met abonnementen gewerkt wordt. De verwerking van persoonsgegevens is hierbij AVG-proof gemaakt.

Sportconsultanten organiseren vaak stadsbrede evenementen. Mensen moeten zich daarvoor aanmelden, vaak met persoonsgegevens. Voor het gebruik van de gegevens wordt om toestemming gevraagd.

In de samenwerking met andere partijen (vb. HAN-bus voor een gezondheidscheck), waarbij persoonsgegevens opgeslagen worden, blijft het goed opletten. Wie is eindverantwoordelijk voor AVG? Als gemeente blijf je altijd medeverantwoordelijk, al zou het alleen maar voor de uitstraling zijn.

Binnensport

We hebben 30 gemeentelijke binnensportaccommodaties: 1 sport/evenementen hal (beheerd), 5 sporthallen (beheerd), 9 sportzalen (onbeheerd, met code) en 15 gymzalen (onbeheerd, met code). De leidinggevende gaf aan nauwelijks tot geen problemen rondom AVG te hebben. Er is contact met huurders over bv. annuleringen en verbouwingen. Dit is de boeker van de activiteit, geeft regelmatig persoonsgegevens op. Hier is verder weinig gedoe mee. Vraag is wel: mogen we een actieve uitnodiging sturen naar huurders, zoals voor een besprekavond? De FG en PO raden aan bij nieuwe huurders eenmalig expliciet toestemming te vragen voor het gebruik van gegevens voor insprekavonden en dergelijken.

Er zijn daarnaast twee ontwikkelingen die aandacht vragen:

- Bij de ontwikkeling van narrowcasting bij binnensport: (mede op onbeheerde locaties) communiceren met huurders via beeldschermen om te laten zien wat er op de sportlocaties gebeurt en mensen welkom te laten voelen bij binnenkomst. Als je automatisch gegevens van een club laat zien moet het geen probleem zijn, maar als iemand onder zijn/haar privénaam heeft aangemeld, kan je een datalek krijgen.

	<p>- Steeds vaker wordt gevraagd om het filmen van trainingen, vanuit een centraal geregelde camera-installatie/livestreams. Gaan we dit faciliteren? Waar ligt verantwoordelijkheid wat betreft AVG? Leg je deze zorg dan bij de verenigingen neer, of zijn wij eindverantwoordelijk? Wat als één leerling niet gefilmd wil worden?</p> <p>Buitensport Het meeste werk van buitensport verloopt digitaal. Het contact dat buitensport heeft, is voornamelijk dat met hoofdaanemers, bedrijven en verenigingen. Voor de eerste twee partijen geldt dat hier meestal gecontacteerd wordt met bedrijfsadressen. Bij verenigingen komt het wel voor dat er privé-contactgegevens worden gebruikt. Verder is er incidenteel contact met particuliere gebruikers van sportparken, bijvoorbeeld bij vernieling.</p> <p>Bij het gebruiken en doorsturen van gegevens wordt altijd om toestemming gevraagd. Gegevens komen vaak uit een huurovereenkomst, waar men voor heeft ingestemd dat het contact voor dat doeleinde gebruikt mag worden. Bij de vanuit het verleden al lopende contracten is geen 'inhaal'-check gedaan.</p> <p>Er is regelmatig contact tussen de leidinggevende en de privacy-ambassadeur, waardoor acties rondom AVG ondernomen zijn en onder de aandacht blijft.</p> <p>Bijzonderheden: - In afgelopen jaren waren er contactgegevens van kampeerders voor de 4-daagse camping. De camping is nu gestopt, de bestanden met contactgegevens zijn verwijderd. - Krachthonk: de gegevens hiervoor worden vastgelegd in ons systeem voor toegangspassen. Als iemand een jaar + kwartaal (bedenktijd voor klanten) geen lid meer is worden, wordt deze automatisch uit het systeem verwijderd. Het is een systeem dat offline werkt.</p>
Systemen totaal	<ul style="list-style-type: none"> - AMIS - CODA - Excel - Outlook - iPhone - Social media voor Jan Massink Hal - G-schijf - Gemeenschappelijke schijf
Belangrijkste risico's	<ul style="list-style-type: none"> - Contacten met inwoners met een sportvraag of sportdeelname. - Het gebruik van telefoonnummers in WhatsApp. - Samenwerking met andere partijen: welke partij verantwoordelijk voor AVG? - Toekomst: narrowcasting op binnensportlocatie: hoe veiligheid goed in te regelen? - Toekomst: filmen trainingen. Hoe zorg je dat dit AVG proof gebeurt?
Mogelijke acties	<ul style="list-style-type: none"> - Er zijn vragen bij sportontwikkeling n.a.v. AVG-modules op Studytube: wat moet je doen met gegevens in de mail en de mappen? Wat wordt verwacht en wat is werkbaar? Er is behoefte aan uniforme afspraken voor de afdeling. - Mail privacy ambassadeur VSA over verwerkingsovereenkomsten voor sportontwikkeling. Leidinggevende had nog wat vragen of wanneer je dit moet toepassen. Hoe werkt het in de praktijk? Moet op toegezien worden. - Opstellen aantal handige standaard AVG-zinnen voor het opstellen van contracten en omgaan met contacten. - Verkennen monitoringssysteem Sportkompas (landelijke dag waar leidinggevende sportontwikkeling was) en ticketsysteem Stadsbeheer (uit gesprek met FG en PO).

Accommodaties	
Globale stand van zaken	<p>Accommodaties kent de volgende takken: wijkcentra, recreatie (Leemkuil, Brakkefort, Triavium), wijkspelaarten en kinderboerderijen.</p> <p>Wijkcentra Er worden veel (huur)gegevens in ordners bewaard, staan niet altijd in afgesloten ruimten. Ook is er los contact tussen beheerders en inwoners. Er kunnen bv. telefoonnummers uitgewisseld worden. Niet duidelijk hier altijd expliciet toestemming voor nodig is. Verder levert een scan door de map van wijkcentra op dat er klantnummers in te lezen zijn, soms met persoonsgegevens.</p> <p>Bij de verhuurbalie wordt via AMIS veel gebruik gemaakt van persoonsgegevens. Zie BOVSA.</p> <p><i>Vrijwilligers:</i> als vrijwilligers zich aanmelden, vullen zij met een beheerder een aanmeldformulier in. Deze wordt goedgekeurd door de teamleider en doorgestuurd aan de vrijwilligerscoördinator van het secretariaat. Deze coördinator vraagt de VOG aan, scant het aanmeldformulier in en verwijdert het papieren document, zodat de gegevens nog maar op één plek te vinden zijn. Dat is op de persoonlijke schijf van deze persoon, zodat anderen hier geen toegang tot hebben. De naam, (email)adres, woonplaats, geboortedatum en noodnummer voor de vrijwilliger worden geregistreerd via de vrijwilligersovereenkomst. Hierin staat een vermelding over het gebruik van persoonsgegevens.</p> <p>Recreatie Bij recreatie worden er abonnementen afgesloten met persoonsgegevens, zowel voor het Triavium als voor de stedelijke spelaarten. Dit verloopt via het kassasysteem. Voor meer informatie, zie BOVSA.</p> <p>De huuradministratie van verenigingen verloopt via AMIS (zie BOVSA). Er zijn werkafspraken over hoe met gegevens omgegaan wordt: er wordt om toestemming gevraagd voor het gebruik van de gegevens en er wordt verteld hoe met de gegevens omgegaan wordt.</p> <p>Daarnaast is er contact over kinderfeestjes bij de spelaarten of het Triavium. Dit contact verloopt via de mail. Vervolgens wordt de voornaam en het telefoonnummer van de ouder/contactpersoon bij gehouden in een Excelbestand. Er zijn geen expliciete afspraken gemaakt over het bijhouden van deze gegevens en het verwijderen/anonimiseren van data. Hetzelfde geldt voor schoolfeestjes, wanneer deze door ouders geregeld worden (en er dus persoonsgegevens gebruikt worden).</p> <p>Kinderboerderijen en wijkspelaarten Hier wordt weinig tot geen gebruik gemaakt van persoonsgegevens. Alleen bij de registratie vrijwilligers, zie wijkcentra. Zeer klein risico.</p>
Systemen totaal	<ul style="list-style-type: none"> - AMIS - Planon - Kassa's - Facilitator (Heyday) - Word - Outlook - CODA - iPhone - G-schijf - Gemeenschappelijke schijf
Belangrijkste risico's	<ul style="list-style-type: none"> - Ordners in wijkcentra - Verwerken abonnementen en verwijderen gegevens (qua proces goed ingericht) - Huuradministratie

	- Gegevens kinderfeestjes en schoolreisjes
Mogelijke acties	<ul style="list-style-type: none"> - Opschoonactie mappen G-schijf en gemeenschappelijke schijf nodig. - Af en toe bij beheerders AVG onder de aandacht brengen, met name over het veilig bewaren van de ordners. - Afspraken maken over bewaren van persoonsgegevens bij schoolreisjes en kinderfeestjes.

BOVSA	
Globale stand van zaken	<p>BOVSA bestaat uit 5 kolommen: secretariaat, facilitair, managementinformatie, veiligheid en verhuurbalie.</p> <p>Secretariaat Het secretariaat zorgt voor agendabeheer van managers, heeft ook toegang tot mail van hen. Zij versturen mailings (intern/extern) waar persoonsgegevens in voor kunnen komen. Ook regelt het secretariaat de instroom, doorstroom en uitstroom van personeel en hebben zij een bestand met verjaardag, cursussen (NAW-gegevens) etc. Ook leggen zij soms persoonsgevoelige informatie vast en zijn zij beschermer van vertrouwelijke informatie. Het secretariaat heeft dus een redelijk groot risico op AVG-zaken. Aandacht hiervoor is regelmatig nodig.</p> <p>Facilitair Facilitair zorgt voor het contractmanagement van schoonmaak, inkoop horeca, bedrijfskleding nieuwe medewerkers (gegevens maten), leveren procesondersteuning voor de kassa's, regelen aanbestedingen en zorgen voor camerabewaking. Facilitair heeft relatief weinig persoonsgevoelige informatie en daarmee een klein AVG-risico. De kassa's zijn AVG proof ingeregeld.</p> <p><i>Camerabewaking:</i> dit hebben we al jaren, de kwaliteit ervan is teruggelopen. Camerabewaking 'zit' bij niemand, niemand houdt zich hiermee bezig. Een paar jaar geleden was er een offerte, maar daar is uiteindelijk niets mee gebeurd. De AVG rondom de camera's is niet expliciet geregeld. Met de camerabeelden mogen we niet veel, alleen de politie mag dit. Als we er toch niets mee mogen, waarom hebben we ze dan nog? Hier is een besluit over nodig. In 2022 is er naar aanleiding van een NOS-artikel over Chinese camerabewaking onderzocht of we risico hebben op Chinese spionage. Dit risico is zeer klein, aangezien de camera's niet direct aangesloten zijn op internet.</p> <p><i>Kassa's:</i> via de kassa's lopen de abonnementen. Bij de inkoop van de kassa's een aantal jaar terug is AVG goed meegenomen. Voor het afsluiten van de abonnementen is gekeken naar welke informatie minimaal nodig is voor verkoop. Meer informatie wordt niet meer ingevoerd. Iedereen die een abonnement heeft, heeft een klantenkaart in het systeem, waar je een abonnement op kunt laden. De kaart is een pasje en/of QR-code. Daar kan zowel een abonnement voor de speeltuinen als voor het Triavium op. De afspraak is dat alle data worden opgeschoond, als het speeltuin- of schaatsseizoen is afgelopen. Als een jaar (plus net wat meer tijd) niets op de kaart is geladen, wordt de kaart geanonimiseerd. De gegevens blijven in dit systeem, er wordt niets geëxporteerd. Er is verder nog een webshop waar je online een ticket kunt kopen, gekoppeld aan het kassasysteem van de Haan. Ook daar is minimaal een emailadres voor nodig. Op de kassa's zelf zijn de gegevens zichtbaar, bij de backoffice zouden gegevens geëxporteerd kunnen worden. Daar heeft slechts een beperkt aantal mensen toegang. Voor de abonnementenmodule binnen het kassasysteem moet contact opgenomen worden met de PO, om te verkennen of formele DPIA nodig is.</p>

	<p>Managementinformatie Managementinformatie zorgt voor het applicatiebeheer, databeheer en levert een stukje managementinformatie. Zij hebben weinig te maken met (nieuwe) persoonsgegevens, dus klein AVG-risico. Het is vooral de vraag wie welke autorisaties heeft en welke persoonsgegevens kan inzien.</p> <p>Veiligheid Veiligheid zorgt voor de RI&E's (veiligheid personeel) en BHV-trainingen (hierin zitten verwerkingsovereenkomsten). Ook zorgen zij voor gebruikersvergunningen van wijkcentra. RI&Es kunnen persoonsgevoelige informatie hebben, bijvoorbeeld adresgegevens wanneer er agressie plaatsgevonden heeft, maar het risico is klein. De verwerkingsovereenkomsten van de BHV-trainingen moeten wel getoetst worden.</p> <p>Verhuurbalie Voor AMIS is recent een DPIA ingeleverd bij de FG.</p> <p>De verhuurbalie registreert en verwerkt reserveringen van huurders van sportzalen en wijkcentra. Dit zijn soms rechtspersonen, soms natuurlijke personen (waaronder ZZP-ers). Ook zorgt de verhuurbalie voor abonnementen van het Krachthonk en recreatie. Er wordt hier veel gewerkt met persoonsgegevens, dus een relatief groot risico. Aandachtspunten: verwerkingsovereenkomsten en controles daarop, opschonen data (welke gegevens niet meer nodig), toegang GBA (gegevens natuurlijke personen). Daarnaast is een check nodig op AMIS + AB-debiteuren: wie kunnen nog bij de data en is dat nodig?</p> <p>Zaken worden in AMIS niet automatisch geanonimiseerd. Dit zou je bijvoorbeeld 1x per jaar moeten doen voor huurders die al twee jaar niet meer huren (en waar je ze dus niet meer voor het primaire doel 'huren' nodig had). Hier zouden we beleid/richtlijnen voor op moeten stellen en een werkproces voor moeten inrichten. Zodat je hier ook op kunt verantwoorden.</p> <p>AMIS is gekoppeld met CODA voor betalingen. Dit gebeurt alleen op basis van een factuur. Aan CODA zitten BRP en KvK-gegevens. Bij het 0-tarief gebeurt dit niet. Soms betalen deze 0-tarievers wel voor koffie/thee, maar dit gaat per kas, niet via CODA.</p> <p>Vanuit AMIS worden mailings gestuurd, dit wordt ge-cct naar de verhuurbalie. Daar kunnen ook persoonsgegevens in zitten.</p> <p>Bij de huur voor sport kunnen huurders zelf boeken via AMIS online. Gegevens, zoals de boekgeschiedenis worden hierbij opgeslagen. Hier komt nog 2-factoridentificatie voor, zodat gegevens beter beschermd zijn. Dit is breder dan alleen privacy, gaat om informatieveiligheid in het algemeen.</p> <p>Daarnaast worden vanuit AMIS allerlei uitdraaien gemaakt. Moet en mag je dit bewaren of moet dit op een gegevens moment weg?</p> <p>Planon is voor verhuur van vastgoed. Daarin wordt vaak meer vastgelegd dan strikt noodzakelijk. Hoe lang bewaar je gegevens? Ook dit is gekoppeld aan CODA.</p> <p>De gemeente houdt informatieprocessen bij via de Cybermanager. In dit systeem zouden we kunnen kijken naar welke apps gevoelig zijn qua privacy.</p>
Systemen totaal	<ul style="list-style-type: none"> - AMIS - Planon - Kassa's - Facilitator (Heyday) - Word - Outlook - CODA - iPhone - G-schijf

Belangrijkste risico's	<ul style="list-style-type: none"> - Gemeenschappelijke schijf - Gebruik persoonsgegevens bij het secretariaat. - Notulen bij het secretariaat. - Lijsten met verjaardagen, cursussen etc. bij secretariaat. - Camerabewaking (in elk geval voor het imago). - Verhuurbalie: verwerking persoonsgegevens in AMIS en koppeling CODA, ook cc's naar mail. - Verhuurbalie: op tijd verwijderen informatie die verouderd is. - Verhuurbalie sport: automatisch opslaan gegevens kan veiliger.
Mogelijke acties	<ul style="list-style-type: none"> - Secretariaat: inhaalactie toestemming op oude gegevens? Te denken aan bv. verjaardagen: wil je er niet meer in staan, geef het aan. Ook voor adresgegevens voor bijvoorbeeld bloemetjes. - Onboarding: welke toestemmingen geeft een nieuwe medewerker over gebruik persoonsgegevens op de afdeling. - Wat te doen met (verouderde) analyses in mappen? - Besluit over de camerabewaking. FG: er is een DPIA en/of cameraprotocol nodig. - Voor de abonnementenmodule binnen het kassasysteem moet contact opgenomen worden met de PO, om te verkennen of DPIA nodig is.

Staf	
Globale stand van zaken	<p>De staf heeft veel afwisselend werk, met weinig routinematige processen. Daarom moet bij elk project opnieuw afgewogen worden waar afspraken rondom AVG gemaakt moeten worden en bekeken worden wat de risico's zijn.</p> <p>Algemene risico's:</p> <ul style="list-style-type: none"> • Opslaan telefoon- en emailadressen in de telefoon en documenten (en af en toe het doorsturen van deze gegevens aan collega's). Hiervoor wordt niet altijd bewust om toestemming gevraagd. Ook wordt informatie bewaard in mails. • In (ontwikkel)projecten waar persoonsgegevens worden gebruikt worden niet altijd expliciet afspraken gemaakt over het gebruik van persoonsgegevens. • Per ongeluk naar een verkeerde persoon mailen. • Af en toe lijsten uit AMIS e.d. Dit wordt dan niet altijd geanonimiseerd en op tijd weggegooid. • Collega's soms inblikrecht in systemen als AMIS en Planon. Hiervoor ligt de primaire verantwoordelijkheid bij de applicatiebeheerders. <p>Specifiek:</p> <p>Het meeste contact via NAW-gegevens loopt via de stafmedewerker die vaak contact heeft over klachten, toegangszeggingen en overige correspondentie met inwoners. Eerder werd deze informatie bewaard. De insteek is nu:</p> <ul style="list-style-type: none"> • Klachten die geregistreerd zijn gaan na behandeling naar het archief; daarnaast bewaart deze collega klachten of meldingen afhankelijk van het type melding/klacht in Citrix, 1 jaar of langer. • Toegangszeggingen zaten in een fysieke map, die map is opgeschoond. Digitaal blijven ze bij de collega bewaard tot de termijn is afgelopen. Op de locatie heeft men

	<p>zelf ook een exemplaar. Bij de rondgang is aangegeven dat die exemplaren weg moeten als de termijn verlopen is.</p> <p>Daarnaast wordt er gewerkt aan het verbeteren van de verhuurprocessen. Zie hiervoor BOVSA.</p>
Systemen totaal	<ul style="list-style-type: none"> - Word - Outlook - CODA - iPhone - AMIS - G-schijf - Gemeenschappelijke schijf
Belangrijkste risico's	- Contact met inwoners: expliciet vragen om toestemming.
Mogelijke acties	- Algemene afspraken maken (zie VSA algemeen) en af en toe het stafoverleg onder de aandacht brengen.

VSA algemeen	
Globale stand van zaken	<p>De indruk is dat er afgelopen jaren al meer aandacht en bewustzijn voor AVG is gekomen en dat er verschillende verbeterlagen zijn gedaan. Deze indrukken zijn op basis van gesprekken en dus hoe men het ervaart. De vraag is of dit strookt met de werkelijkheid. Veel problemen met datalekken zijn de afgelopen jaren niet voorgekomen.</p> <p>Er zijn meerdere vraagstukken naar boven gekomen, zie mogelijke acties.</p> <p>De afgelopen jaren is het belang van DPIA's (data protection impact assessment) steeds meer toegenomen. Dit is een instrument die de FG gebruikt om privacy risico's van gegevensverwerking in kaart te brengen. De afgelopen jaren is dit al vaker gedaan, bijvoorbeeld bij de aanpassingen van het verhuurproces. Voor bestaande processen is vaak geen DPIA gedaan. Het uitvoeren van DPIA's op bestaande processen helpt om verder in control te komen.</p>
Systemen totaal	<ul style="list-style-type: none"> - AMIS - Planon - Atlaz - Gebouwenpaspoort - Dashboard met managementinfo (in ontwikkeling door EI-team, 5.1.2e en 5.1.2e) - Kassa's - Facilitator - Word - Outlook - CODA - iPhone - G-schijf - Gemeenschappelijke schijf
Belangrijkste risico's	<p>De grootste AVG-risico's zitten bij:</p> <ul style="list-style-type: none"> - secretariaat - verhuurbalie - wijkcentra: ordners - assetmanagement - sportontwikkeling
Mogelijke acties	- Opfrisronde bij alle teams: informatie herhalen, dilemma's delen en vervolgacties afstemmen.

	<ul style="list-style-type: none"> - Opschoonactie mappen per bureau: waar zitten nog persoonsgegevens die niet bewaard mogen worden? - Afspraken maken per bureau over wat te doen met analyses: is het nodig om persoonsgegevens te verwerken of kan dit ook geanonimiseerd worden? Als er wel persoonsgegevens nodig zijn: hoe lang bewaar je dit en welke afspraken maken we over bewaartermijnen en de verantwoordelijken hiervoor? - Afspraken maken per bureau over archivering van data: hoe voorkom je dat er onnodig persoonsgegevens opgeslagen worden? - Afdelingsbrede afspraken over opschonen van mail en telefoon. Dit is een vraagstuk dat voor de gehele gemeente geldt. - Afspraken over vervolg: hoe houd je AVG up to date? Bijvoorbeeld jaarlijks moment kiezen om dit bestand te updaten en vervolgacties af te stemmen. - Het uitvoeren van DPIA's op huidige werkprocessen.
--	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Legenda toegepaste uitzonderingsgrondslagen

In dit document zijn gegevens geanonimiseerd op grond van:

Wet	Artikel	Omschrijving	Pagina's
Wet open overheid	Art. 5.1 lid 2 sub e	De eerbiediging van de persoonlijke levenssfeer	11