Amersfoort
GEMEENTEBLAD
Officiële uitgave van de gemeente Amersfoort
Nr. 106260
15 maart
2023

Privacybeleid Gemeente Amersfoort 2019

Definities en afkortingen

AVG: Algemene Verordening Gegevensbescherming.

Autoriteit Persoonsgegevens (AP): is de onafhankelijke toezichthouder in Nederland die de bescherming van persoonsgegevens bevordert en bewaakt.

Betrokkene: de persoon op wie de persoonsgegevens betrekking hebben. De betrokkene is degene van wie de gegevens worden verwerkt.

CISO (Corporate Information Security Officer): functionaris met een adviserende, coördinerende en toezichthoudende rol op het gebied van Informatiebeveiliging. Hij ziet er op toe dat de informatieveiligheid in de gemeentelijke organisatie voldoet aan de hiervoor geldende normen.

DPIA (Data Protection Impact Assessment): in een vroeg stadium op een gestructureerde en heldere manier in beeld brengen wat de privacyrisico's van een verwerking zijn en welke maatregelen getroffen dienen te worden aan de hand van de geconstateerde risico's. Een DPIA is verplicht bij een nieuwe verwerking of bij een bestaande verwerking als het risico of het proces wijzigt.

DNA: staat voor Dichtbij, Nieuwsgierig en Aanspreekbaar en vormen de (ambtelijke) kernwaarden van de organisatie.

Externe partijen: de formeel verbonden partijen, zoals bedoeld in het Besluit Begroting en verantwoording; een Publiek Private Samenwerking en Gemeenschappelijke Regeling en partijen waaraan de gemeente Amersfoort een subsidie heeft verstrekt en/of opdracht heeft verleend en die van zwaarwegend belang zijn voor de gemeente Amersfoort.

FG (Functionaris Gegevensbescherming): (interne) toezichthouder op de verwerking van persoonsgegevens.

Persoonsgegevens: alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon. Dit betekent dat informatie ofwel direct over iemand gaat, ofwel naar deze persoon te herleiden is. Gegevens van overleden personen of van organisaties zijn geen persoonsgegevens volgens de AVG.

Privacy by design / default: Privacy by design houdt in dat al bij het ontwerpen van een proces of systeem gegevensbescherming al is meegenomen zodat persoonsgegevens goed worden beschermd en de gegevens niet langer worden bewaard dan nodig is voor het doel van de verwerking. daarnaast moeten de standaardinstellingen voor een gebruiker zo privacy-vriendelijk mogelijk zijn ingesteld (Privacy by default).

Stelselhouder: voor het laten werken van het stelsel is de afdeling JDA aangewezen als Stelselhouder Privacy. De Stelselhouder is verantwoordelijk voor de centrale sturing en regie, door onder meer kaderstelling via beleidsvoorstellen, monitoring van de compliance (tweede lijn).

Toestemming: elke vrije, specifieke, geïnformeerde en ondubbelzinnige wilsuiting waarmee de Betrokkene door middel van een verklaring of een ondubbelzinnige actieve handeling een hem betreffende verwerking van persoonsgegevens aanvaardt.

Verwerken: Een verwerking is volgens de AVG elke bewerking of elk geheel van bewerkingen met betrekking tot persoonsgegevens. Veel voorkomende bewerkingen zijn: verzamelen; vastleggen; opslaan; wijzigen; opvragen; raadplegen; gebruiken; verstrekken; wissen en vernietigen.

Verwerker: de persoon of organisatie die ten behoeve van de verwerkingsverantwoordelijke persoonsgegevens verwerkt.

Verwerkingsverantwoordelijke: een persoon of instantie die, alleen of samen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt. De bestuursorganen van de gemeente zijn allemaal verwerkingsverantwoordelijken voor de verwerkingen die door of namens de gemeente worden uitgevoerd. De verwerkingsverantwoordelijken zijn onder andere de burgemeester, het college van burgemeester en wethouders en de gemeenteraad.

I – Inleiding

De gemeente Amersfoort vindt privacy belangrijk. Dat betekent dat wij met aandacht en respect voor de privacy van bewoners en medewerkers ons werk doen. Hierom stellen we een Privacybeleid vast. Ook de wet (de Algemene Verordening Gegevensbescherming, hierna: AVG) schrijft voor dat een gemeente een Privacybeleid heeft. Daarmee maken we ons handelen transparant en nemen wij verantwoordelijkheid. Het beleid is geschreven voor onze burgers, onszelf en onze medewerkers en ziet op de (onderdelen van de) gemeente Amersfoort als bestuursorgaan en als werkgever.

Dit Privacybeleid van de gemeente Amersfoort is de opvolger van het Privacybeleid 2017-2019 en incorporeert de inmiddels van kracht geworden AVG. Dit nieuwe Privacybeleid beschrijft de context van het beleid, de doelen en de uitgangspunten voor ons handelen. Daarmee maken we inhoudelijke keuzes binnen de kaders van de AVG en verwante regelgeving.

Het Privacybeleid is gebaseerd op de volgende (bestuurlijke) uitgangspunten en gemeentelijke kernwaarden. Deze uitgangspunten en waarden versterken elkaar.

A. We zetten de mens centraal bij onze verwerkingen: wat we doen, doen we voor de burger. We zijn transparant over onze verwerkingen zodat iedereen weet waar hij aan toe is, vragen input van en luisteren naar de burger.
B. De uitvoering van wettelijke taken van de gemeente, optimale dienstverlening en privacybescherming betekenen het constant zoeken naar een evenwichtige balans. De gemeente Amersfoort streeft naar een optimum, met risico oriëntatie en het moreel kompas als belangrijke ijkpunten. We geloven dat een goede privacybescherming, dienstverlening en werkbaarheid samen kunnen gaan. Waar dit botst en privacy moet wijken voor de uitvoering van onze taken, of omgekeerd, maken we de besluitvorming hierover transparant.
C. Veiligheid is een randvoorwaarde, zowel bij de verwerking van persoonsgegevens als bij de werkomgeving van onze medewerkers.
D. Juiste grondslag. We verwerken persoonsgegevens in beginsel op basis van grondslagen die bij onze rol als overheid horen (Wettelijke verplichting, taak van Algemeen belang en / of in het kader van een taak van Openbaar gezag) en verwerken bij voorkeur niet op basis van de rechtsgrond Toestemming.

Het herziene beleid heeft geen vaste looptijd. Wel vindt evaluatie plaats in 2022, gelijktijdig met de herziening van het Informatiebeveiligingsbeleid.

II – Achtergrond van het Privacybeleid

Met dit Privacybeleid wil de gemeente Amersfoort de verwerking van persoonsgegevens rechtmatig en op een effectieve wijze laten plaatsvinden. Daarbij zijn de volgende aspecten relevant voor dit herziene beleid.

1. Voldoen aan (gewijzigde) wettelijke eisen

Het bestaande Privacybeleid was toe aan herziening. De invoering van de AVG heeft de wettelijke eisen aan Privacy aangescherpt. Het beleid van 2017 dient geactualiseerd te worden.

2. Beleid voor een nieuwe fase

Nu de AVG inmiddels meer dan een jaar geldt, is een nieuwe fase aangebroken, waarin behoefte bestaat de ruimte te nemen die de wet- en regelgeving bieden om onze taken effectief en efficiënt te vervullen en tegelijkertijd burgers met respect, eerlijk en begripvol te behandelen.[1] Daarbij ontstaan (ethische) dilemma's. De (nationale) wet- en regelgeving is namelijk complex en biedt niet altijd voldoende houvast aan lokale beleidsmakers en –uitvoerders bij de uitvoering van hun taken. Verder heeft het recht op bescherming van persoonsgegevens geen absolute gelding en moet worden beschouwd in relatie tot de functie ervan in de samenleving. Dat vraagt soms afweging tegen andere (grond)rechten, bijvoorbeeld in het sociaal domein, waar de raad ons een opdracht heeft gegeven om integraal en domeinoverschrijdend te werken. Sommige opdrachten kunnen met elkaar botsen en soms voldoen bestaande (IT-)systemen en werkwijzen nog niet aan de privacy- en informatiebeveiligingseisen.

Privacy vraagt daarmee niet alleen om een heldere bestuurlijke visie op privacy maar ook om duidelijke beleidskaders. Privacywetgeving, waaronder de AVG, biedt niet voor ieder vraagstuk een pasklaar

1) Onderzoek van Kantar voor de Nationale Ombudsman over de relatie tussen de overheid en de burger in 2030, publicatiedatum 11 juli 2019. https://www.nationaleombudsman.nl/system/files/bijlage/1%20RAPPORT%20Nationale%20Ombudsman%20-%20relatie%20burger%20overheid%202030_def.pdf

antwoord maar schept juist ruimte door regels in de vorm van principes te formuleren waar aan moet worden getoetst wanneer gegevens verwerkt worden. Deze regels kunnen vaak verschillend worden ingevuld of toegepast.[2] Een belangrijk onderdeel van het herziene beleid is aandacht voor risico oriëntatie en het moreel kompas: de wet is een belangrijke leidraad, maar bij handelen conform de regels of gebruikmaken van de (wettelijke) ruimte, hoort een gewetensvraag: ook al houd ik me aan de regels, is deze oplossing ook in maatschappelijk opzicht wenselijk?[3] Of op de juiste wijze invulling is gegeven aan deze principes en voldoende waarborgen zijn getroffen om de persoonlijke levenssfeer te beschermen is aan de toezichthouder en aan de rechter. De gemeente Amersfoort wil met dit beleid de ruimte benutten die er is om haar taken goed uit kunnen voeren en de privacy van betrokkenen beschermen. Waar dit schuurt maken wij dat transparant. Verantwoording afleggen vinden wij horen bij een betrouwbare overheid.

3. Incorporatie van een goede privacybescherming in werkzaamheden organisatie

Uit het voorgaande moge duidelijk zijn dat er onduidelijkheid kan zijn over de eisen die wet- en regelgeving stellen. Dit kan tot onzekerheid leiden en medewerkers kunnen zich gehinderd voelen om hun taken uit te voeren en of privacy ervaren als een vervelende extra check bij reguliere processen. Anderen voeren – vaak ten onrechte – privacyregels juist aan om informatie niet te delen. Iets om je achter te verschuilen. Iedereen is het er echter over eens dat van ons als gemeente verwacht mag worden dat we met aandacht voor de bescherming van privacy ons werk doen. Dit beleid beoogt om de professionals op de werkvloer in staat te stellen afwegingen te maken bij de uitvoering van het werk. We willen dat rechtmatige verwerking van gegevens geen extra belastende handeling vormt maar onderdeel is van de reguliere taken en processen.

4. (Bijdragen aan de ontwikkeling) Privacy governance

In de gemeentelijke organisatie zijn de bevoegdheden zo laag mogelijk in de organisatie belegd waarbij iedereen verantwoordelijkheid draagt voor zijn eigen taakveld, op basis van vertrouwen. Dat betekent ook dat afwegingen rond privacy, zeker als deze meer en meer onderdeel worden van de reguliere taken en processen, ook gemaakt (zullen) worden op uitvoerend niveau. Om dit soort afwegingen te kunnen maken en uit te kunnen leggen (transparantie) is een afwegingskader nodig. Hier is ook behoefte aan.

Verder is nodig om onze privacy governance te herijken en in het Privacybeleid duidelijkheid te maken wie waarvoor verantwoordelijk is. We hebben een stelselhouder (JDA) en een FG maar ook verschillende afstemmingsstructuren.[4] Met het creëren van duidelijkheid borgen we privacy in de bedrijfsvoering en kunnen we deze verbinden met de cyclus van permanent verbeteren. Dat doen we ook door jaarlijks een Privacyplan op te stellen.

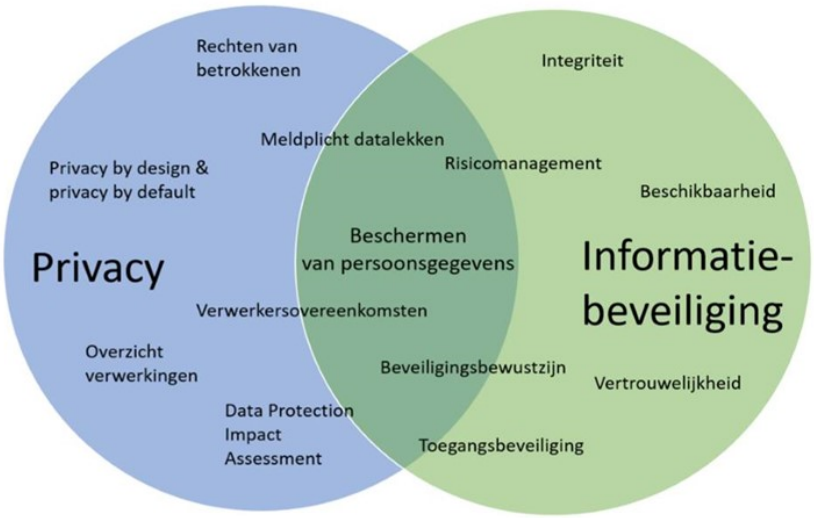
III – Context en reikwijdte

Dit beleid gaat over de verwerking van persoonsgegevens, hierna gemakshalve 'privacy'. Het Privacybeleid heeft geen geografische begrenzing; de uitgangspunten van het beleid binden (de bestuursorganen van) de gemeente Amersfoort bij haar handelen, ook wanneer sprake is van Verwerkers of samenwerking. Diezelfde uitgangspunten vormen derhalve het kader bij de selectie van leveranciers c.q. Verwerkers, bij het maken van afspraken met hen en dat we er bij de uitvoering van de werkzaamheden aan toetsen. Het beleid is ook van toepassing in geval van uitwisseling van informatie met andere gemeenten en organisaties bij de uitbesteding van publieke taken aan Externe partijen. Bij het maken van afspraken met (Externe) partijen worden inhoud en vorm van onze afspraken bepaald aan de hand van het (politieke, bestuurlijke dan wel juridische) risico van de verwerking, alsmede de positie die deze partij in relatie tot de gemeente Amersfoort inneemt.[5]

Voorts betekent dit dat het beleid zich ook uitstrekt over de verwerkingen van persoonsgegevens op grond van de wet Basisregistratie Personen (BRP) en op de verwerkingen waarop de Archiefwet van toepassing is. Uiteraard voor zover deze specifieke wet- en regelgeving geen afwijkende eisen stellen.[6]

2) Daarvoor is een aanpak nodig die lijkt op risicomanagement, een aanpak van 'pas toe of leg uit'. Hoewel er ook verschillen zijn omdat privacy uiteindelijk een integriteitsaangelegenheid is (moraliteit).
3) Immers, ook als je binnen de wet opereert, compliant daarmee bent, kan wat je doet en besluit onaanvaardbaar of schadelijk zijn. Keynote, De juiste antennes voor good governance, Marry de Gaay Fortman bij de Goed bestuur jaarlezing d.d. 15 mei 2019.
4) Sleutelpersonen, Kerngroep en werkgroep, SIO-overleg.
5) Er kan sprake zijn van een gezamenlijke verantwoordelijkheid voor de verwerking, of partijen die taken voor ons uitvoeren in mandaat.
6) Persoonsgegevens mogen alleen o.b.v. de Archiefwet worden bewaard als deze in overeenstemming met de AVG zijn verzameld. Voor het archiveren en bewaren wordt specifiek beleid opgesteld. Verwerkingen op basis van de wet BRP kennen een eigen regime dat minimaal gelijk is aan of strenger is dan de AVG-regels.

Het Privacybeleid hangt samen met het **Informatiebeveiligingsbeleid**, waarbij de beleidsvelden samenkomen rond de **beveiliging** van persoonsgegevens. Deze relatie is visueel als volgt:



Zoals gezegd bevat de privacy wet- en regelgeving veel open normen. Het beleid kan daarom niet helemaal uitgeschreven worden. Daarnaast wil de gemeente Amersfoort dat privacy een onderdeel is van de afwegingen die professionals maken, waarbij bewustwording en de eigen afweging van professionals in de uitvoering leidend is. Dit beleidsdocument bevat daarom onze uitgangspunten en kernwaarden die we waar mogelijk uitwerken. Verder biedt dit Privacybeleid richting voor uitwerking (beleid, procedures, werkinstructies etc.) op deelonderwerpen, waar dat mogelijk en nodig is. Uitwerking gebeurt in elk geval voor de volgende thema's:

- Privacy by design en default
- Archiveren en bewaren / retentiebeleid
- Gebruik / inzet van camera's
- Datalekken
- DPIA's
- Rechten van betrokkenen
- Smart Cities

IV - Uitgangspunten en kernwaarden

De hiervoor genoemde uitgangspunten en kernwaarden van het Privacybeleid van de gemeente Amersfoort worden in deze paragraaf uitgewerkt, zo mogelijk naar een concreet handelingsperspectief of naar maatregelen, waardoor we ons beleid toetsbaar en meetbaar maken.

Het betreft de volgende uitgangspunten en kernwaarden

A. We zetten de mens centraal bij onze verwerkingen: wat we doen, doen we voor de burger.
B. De uitvoering van wettelijke taken van de gemeente, optimale dienstverlening en privacybescherming betekenen het constant zoeken naar een evenwichtige balans tussen bescherming van persoonsgegevens, dienstverlening en werkbaarheid.
C. Veiligheid is een randvoorwaarde, zowel bij de verwerking van persoonsgegevens als bij de werkomgeving van onze medewerkers.
D. Juiste grondslag en bij voorkeur geen verwerking op basis van de rechtsgrond Toestemming.

A – We zetten de mens centraal

De gemeente Amersfoort wil dat mensen zich ongehinderd kunnen ontplooien, terwijl privacy en digitale rechten worden beschermd. Dat is een voorwaarde voor vertrouwen en inclusiviteit. De gemeente Amersfoort wil daarnaast een betrouwbare overheid zijn, die luistert naar de burgers en dichtbij hen staat, weet wat hen beweegt en die aanspreekbaar is op haar handelen. Voor ons handelen betekent dat het volgende.

We geven Betrokkene zoveel mogelijk regie op eigen gegevens

We vinden de regie die Betrokkenen hebben op hun gegevens ('informationele zelfbeschikking') een belangrijk uitgangspunt. Daarvoor is (onder meer) informatie nodig en zijn we transparant waar dat kan:

- Bij nieuwe verwerkingen informeren we Betrokkenen direct en in begrijpelijke taal voor welke rechtmatige, gerechtvaardigde doelen wij hun persoonsgegevens verwerken, in elk geval via onze Privacyverklaring of met een folder.
- We doen geen geheime verwerkingen: al onze verwerkingen staan in ons Register van verwerkingen.
- We vertellen het als we persoonsgegevens verder verwerken dan waarvoor we de gegevens hebben gekregen. Zo vertellen we Betrokkenen als we gegevens op basis van het beginsel 'Eenmalige verstrekking, meervoudig gebruik', vaker zullen gebruiken.
- We publiceren vier keer per jaar een geactualiseerd Register van verwerkingen. Ook maken we daarin openbaar als we een DPIA hebben gedaan.
- We maken datalekken en de afhandeling daarvan openbaar.
- We doen niets met persoonsgegevens wat we zelf niet snappen of niet kunnen uitleggen.[7]
- Als wij geen verantwoordelijke zijn voor een verwerking, maar wel weten wie dat is, verwijzen wij door.[8]
- Als we persoonsgegevens van burgers (moeten) delen bespreken we dat met hen. Maar in sommige situaties (bijvoorbeeld in het zorg- en veiligheidsdomein), kan het nodig zijn over burgers te praten. We maken dan een expliciete afweging, die we vastleggen.
- Als Betrokkenen vragen hebben, dan beantwoorden we die snel en we honoreren hun rechten binnen de kaders van de AVG (aanspreekbaar van DNA).

We geven Betrokkenen inspraak bij verwerkingen die hen in overwegende mate raken (dichtbij van DNA), bijvoorbeeld door hen te raadplegen bij DPIA's.

We zijn voorspelbaar
Ons handelen is voorspelbaar en past bij onze rol als gemeentelijke overheid. Dit betekent het volgende.

- We zijn wel nieuwsgierig, (nieuwsgierig van DNA) maar we koppelen geen gegevens zonder concrete aanleiding of om interessante verbanden te vinden.
- We willen gebruik maken van gegevens en staan open voor innovatieve toepassingen, maar we hoeven niet op de troepen vooruit te lopen. Daarom:
  - Benutten we landelijke (VNG-)modellen (bijvoorbeeld bij DPIA's en verwerkersovereenkomsten).
  - Doen we alleen mee aan pilots als vooraf toetsing aan het Privacybeleid heeft plaatsgevonden en we maken vooraf de risico's van de verwerking van persoonsgegevens inzichtelijk, door een quick scan of door een DPIA.
- We gebruiken persoonsgegevens niet voor commerciële doelen en handelen rechten van Betrokkenen centraal af.

B – Balans: Goede privacybescherming, optimale dienstverlening en werkbaarheid
Gegevensverwerking is nodig bij onze (wettelijke) taakuitvoering en dienstverlening. Een goede borging van privacy is daar onderdeel van. Een goed inzicht in onze gegevens, de organisatie en het beheer daarvan is niet alleen verplicht, maar ook hoe wij vinden dat het hoort. Een goed ingericht gegevensbeheer levert meerwaarde op, bijvoorbeeld voor de continuïteit als er iets mis gaat (zoals een hack of ransomware), voor onze bedrijfsvoering (terugvindbaarheid, archivering en fysieke archiefruimte) en het vertrouwen dat onze inwoners en medewerkers in ons kunnen stellen.
Binnen de ruimte van de privacywet- en regelgeving, verrichten we onze taken. Dat doen we vanuit onze kernwaarden (DNA). Onze taken zijn in beweging en we hebben een grote veranderopgave. De wettelijke regels zijn daar (nog) niet op toegerust. En dat vraagt soms dat we op de rand of buiten de kaders van de regels treden. Dat doen we risico georiënteerd, met inachtneming van ons moreel kompas en we maken het transparant. Medewerkers in relatie tot afdelingsmanagers, net zoals managers in hun managementverantwoording. We kunnen het uitleggen en er verantwoording over afleggen. Dat vinden wij horen bij een betrouwbare overheid. Daarbij nemen we onze verantwoordelijkheid: we zetten de mens centraal, zijn transparant en we doen het veilig. Dat geldt zowel voor het bestuur, de directie, managers als voor individuele medewerkers.

Als privacyregels onevenredige belemmeringen vormen voor de werkbaarheid durven we die ter discussie te stellen: intern door bijvoorbeeld een medewerker bij zijn afdelingsmanager, door een afde-

7) Dat betekent bijvoorbeeld dat we weten of hebben getest hoe onze algoritmes werken en adviezen of beslissingen herleidbaar zijn.
8) Bijvoorbeeld bij camera's in de openbare ruimte.

lingsmanager bij de directie en zo nodig via de burgemeester of het college van burgemeester en wethouders. Extern: bij Betrokkenen en de Autoriteit Persoonsgegevens en desnoods via een gerechtelijke procedure om duidelijkheid van de rechter te krijgen. Indien blijkt dat er geen of onvoldoende rechtsgronden zijn voor het bereiken van bepaalde doelen, dan trekken we aan de bel bij de wetgever.

Bij optimale dienstverlening hoort eenmalige uitvraag, meervoudig gebruik. Dit is al verplicht bij zogenaamde authentieke gegevens uit de basisregistraties. Hergebruik van gegevens gebeurt met inachtneming van de AVG en het Privacybeleid.

C – Veiligheid als randvoorwaarde
Onze betrouwbaarheid als gemeente omvat eveneens de borging van de veiligheid van persoonsgegevens, zowel van onze burgers, onze medewerkers als van de werkomgeving. Dit betekent het volgende.

We brengen privacyrisico's vooraf in kaart en treffen zo beperkende maatregelen
– We voeren op al onze verwerkingen van persoonsgegevens met een hoog risico - een risico analyse (quick scan) uit en waar nodig, vanwege het risico, een DPIA. We treffen maatregelen om de risico's tot een aanvaardbaar niveau terug te brengen.
– We borgen de principes van 'Privacy by design en default' in onze processen (zoals het Demand-supply proces; Architectuur proces; Inkoop proces; Contractproces) en onze Projectdocumentatie (AGPM). We werken dit uit in het deelbeleid voor Privacy by design en default.

We hebben zicht op onze Externe Partijen en relaties en managen de relatie met hen
– We hebben inzicht in onze Verwerkers en hebben verwerkersovereenkomsten met alle Verwerkers conform een landelijke standaard, waarin staat dat zij zich moeten houden aan onze beveiligingseisen. Iedere afdeling heeft een plan om de Verwerkers hierop regelmatig te controleren.
– We beoordelen periodiek de risico's in de relatie met de Externe Partijen en leveranciers.

Onze werkomgeving is veilig en de uitgangspunten zijn helder
– We maken allemaal fouten en iedereen mag fouten maken. We stimuleren onze medewerkers om te leren en bij een datalek lossen we het met elkaar op, maar het is niet vrijblijvend. We stimuleren een lerende omgeving en spreken elkaar aan waar nodig.
– We hanteren het uitgangspunt van een 'passende bescherming'. We werken dit onder meer uit in het deelbeleid voor Privacy by design en default.
– We zorgen ervoor dat onze medewerkers veilig met persoonsgegevens kunnen werken. En dat de implementatie van regels en de uitvoering werkbaar zijn. We betrekken onze medewerkers aan de voorkant, tijdens het proces en aan de achterkant.
– Al onze nieuwe gegevensverwerkingen voldoen aan de geldende informatiebeveiligingseisen; voor alle bestaande gegevensverwerkingen maken we inzichtelijk of deze voldoen aan de eisen en zo nee, maken we een concreet en haalbaar plan om dit op orde te brengen.

D – Juiste grondslag
Voor de verwerking van persoonsgegevens zijn een doel en een grondslag (rechtsgrond) nodig. We starten pas met een verwerking als het doel en de juiste grondslag bekend zijn.

De zes AVG-grondslagen zijn: Toestemming, Wettelijke verplichting, Overeenkomst, taak van Algemeen belang of een taak in het kader van de uitoefening van Openbaar gezag, Vitaal belang en Gerechtvaardigd belang. Voor iedere grondslag gelden bepaalde voorwaarden en bij verwerkingen door de overheid zijn bepaalde grondslagen niet mogelijk of kwetsbaar. We kiezen ervoor te verwerken op basis van grondslagen die bij onze rol als overheid passen, d.w.z. de grondslagen Wettelijke verplichting, taak van Algemeen belang en / of in het kader van een taak van Openbaar gezag. De grondslag Gerechtvaardigd belang gebruiken we alleen als we niet handelen als overheid.[9] We hanteren de grondslag Toestemming liever niet, omdat er bijna altijd sprake is van een afhankelijkheidsrelatie en Toestemming dan niet geldig is.
Als we de grondslag Toestemming gebruiken, geven we alle informatie opdat die Toestemming vrij en op informatie gebaseerd is. Ook over de dan reeds voorzienbare verdere verwerkingen.

We maken uitsluitend gebruik van 'opt out- toestemming' als dit noodzakelijk is voor een goede uitvoering van taken, in bijzonder in het sociaal domein en dit voldoet aan de volgende voorwaarden:

- We doen dit enkel daar waar sprake is van strijdigheid [tussen de bedoeling] van twee wetten [bijv. de Wmo 2015 en de AVG]
- We doen dit enkel na zorgvuldige afweging en besluitvorming in het college
- We beperken eventuele consequenties zo veel mogelijk en communiceren hier transparant over.

9) Bijvoorbeeld als we handelen als werkgever.

V – Meten / jaarplan

Jaarlijks worden de ambities en doelstellingen voor het komende jaar in een door de directie vast te stellen Privacy-jaarplan opgenomen. Periodiek, in elk geval twee maal per jaar, wordt de realisatie van het plan gemeten.

VI – Governance

Met de inrichting van de organisatie rondom privacy wordt vastgelegd bij wie c.q. waar de verantwoordelijkheden liggen en wie welke taak heeft. Hiermee borgen en beheren we het uit te voeren beleid en implementeren we privacy in de reguliere bedrijfsvoering.

Het Privacybeleid staat niet op zichzelf en maakt onderdeel uit van een reeks aan maatregelen om de bescherming van c.q. de verwerking van persoonsgegevens binnen en door de gemeentelijke organisatie te optimaliseren. De bescherming van privacy is een inherent onderdeel van ieders functie / van ieders dagelijks handelen. Tegelijkertijd is de bescherming van persoonsgegevens niet de kerntaak van de meeste medewerkers. Er zijn daarom rollen en functies met adviserende of en toezichthoudende taken op het gebied van privacy en er zijn structuren die deze rollen richten en ondersteunen.

Bij de privacy *governance* gelden de volgende uitgangspunten:

- De gemeente Amersfoort voldoet aan de wettelijke / landelijke eisen die aan privacy worden gesteld, dat betekent onder meer dat de gemeente een Functionaris Gegevensbescherming heeft en dat (wettelijk) verplichte audits worden uitgevoerd.
- De principes van horizontaal toezicht, waarbij de gemeenteraad de eerste controleur is van het college van burgemeester en wethouders; dat betekent dat de gemeenteraad in positie gebracht moet worden om deze rol in te vullen door de verantwoording die het college aflegt via de reguliere planning & control cyclus.
- Het college en (voor de wettelijke veiligheidstaken) de Burgemeester zijn bestuurlijk verantwoordelijk, zij verantwoorden zich ten opzichte van de gemeenteraad en stellen de kaders vast.
- De directie is verantwoordelijk, binnen door het college gestelde kaders, voor de uitvoering van het Privacybeleid.
- De bescherming van persoonsgegevens is een integraal onderdeel van het werken binnen de gemeente Amersfoort. Iedere medewerker die met persoonsgegevens werkt heeft daarbij een rol. Bij de verantwoordelijkhedenstructuur sluiten we zoveel als mogelijk aan bij de bestaande (management-)structuur, zoals vastgelegd in het organisatiebesluit, in het bevoegdhedenbesluit en in het organisatie- en ontwikkelplan "Werken voor Bestuur en Stad." De manager hanteert hierbij de in het Privacybeleid vastgestelde kaders; bij afwijking of interpretatieverschil met bijvoorbeeld de Stelselhouder of de FG vindt gezamenlijke escalatie plaats naar de directie, portefeuillehouder of het college.
- De eerstelijns verantwoordelijkheid voor privacy ligt bij de afdelingsmanagers en hun Sleutelpersonen; JDA is – als stelselhouder Privacy – verantwoordelijk voor de centrale sturing en regie, door onder meer kaderstelling via beleidsvoorstellen, monitoring van de compliance (tweede lijn). De FG houdt tenslotte toezicht, adviseert over kaders en voert audits uit (derde lijn).[10]
- Privacy en informatiebeveiliging zijn verschillende onderwerpen die ook verschillende deskundigheden vragen. Ze hebben echter wel een grote samenhang en invloed op elkaar. De *governance* van privacy moet aansluiten op de IB-structuur en vice-versa. Dit betekent dat de onderwerpen in beleid, toezicht en rapportage wel als onderscheiden onderdelen worden benaderd, maar dat de aansturing en overleggen gecombineerd worden. De FG en de CISO houden afzonderlijke verantwoordelijkheden, maar werken nauw samen.[11]
- Het laten werken van deze *governance* structuur vereist een samenspel tussen alle betrokkenen, waaronder afdelingsmanagers, sleutelpersonen, privacy-adviseurs, de Gemeentearchivaris, CISO, CIO en de FG. Zij zullen ten opzichte van elkaar dichtbij, nieuwsgierig en aanspreekbaar moeten blijven.
- Afdelingsmanagers zijn verantwoordelijk voor het maken van afspraken met Externe partijen, waaronder de partijen waarbij taken in mandaat zijn neergelegd,[12] inclusief het vastleggen van deze afspraken. Vorm en inhoud van deze afspraken worden bepaald door een risicobeoordeling, conform de nota Externe partijen.

10) Voor informatiebeveiliging geldt dezelfde structuur, waarbij ITDA – als stelselhouder –de tweede lijn vertegenwoordigt en de CISO de derde lijn.

11) Hierbij zijn ook de Stelselhouder Privacy, Controller en gemeentearchivaris betrokken.

12) Zoals de Stichting Wijkteams Amersfoort, Indebuurt033, Scholen in de Kunst.