EINDHOVEN GEMEENTEBLAD
Officiële uitgave van de gemeente Eindhoven
Nr. 212262
5 juli
2021

Privacy beleid Gemeente Eindhoven 2020 - 2023

Het college van burgemeester en wethouders van Eindhoven maakt bekend dat zij in haar vergadering van 29 juni 2021 het geactualiseerde Privacy beleid Gemeente Eindhoven 2020 -2023 heeft vastgesteld.

Privacy beleid Gemeente Eindhoven 2020-2023

Colofon

Uitgave
Gemeente Eindhoven
VJB - Veiligheid, Juridische zaken en Bestuur Juridische Zaken
CIO-office

Datum mei 2021

Inhoudsopgave

1. Inleiding

1.1 Algemeen

Iedereen heeft recht op privacy. Privacy wordt in de grondwet “eerbiediging van de persoonlijke levenssfeer” genoemd. Bij privacy gaat het wettelijk gezien om alle gegevens die te herleiden zijn tot een bepaald persoon. Alles wat met die persoonsgegevens wordt gedaan, wordt “verwerken” genoemd (bv. verzamelen, kopiëren, printen, opslaan, publiceren, delen, anonimiseren, bewaren, pseudonimiseren, vernietigen, etc.).

De verwerking van persoonsgegevens is geregeld in de Algemene verordening gegevensbescherming (hierna: AVG). Vanaf 25 mei 2018 wordt er gehandhaafd op basis van de AVG. Het is voor de gemeente belangrijk dat zij haar informatiehuishouding zodanig op orde heeft dat zij voldoet aan de kwaliteitseisen van de AVG. Betrokkenen hebben recht op correcte, veilige en betrouwbare informatieverwerking en moeten erop kunnen vertrouwen dat de gemeente zorgvuldig met deze gegevens omgaat.

1.2 Doel en visie
Doel van dit privacybeleid is het beschrijven van kaders voor het verantwoord omgaan met persoonsgegevens en het waarborgen van de privacy rechten van personen waarvan de gemeente persoonsgegevens verwerkt (of laat verwerken).
De AVG is het centrale kader en houvast voor de wijze waarop we omgaan met persoonsgegevens. Dit beleid is een nadere uitwerking hiervan als uitgangspunt bij de uitwerking van alle aspecten van de gemeentelijke bedrijfsvoering (voor zover hierbij sprake is van de verwerking van persoonsgegevens).

Iedereen werkzaam binnen de organisatie is verantwoordelijk voor het verantwoord omgaan met persoonsgegevens en het waarborgen van de privacy rechten van personen.
We professionaliseren stapsgewijs tot het niveau dat past bij de resultaten van de met dit beleid ingerichte PDCA-cyclus. Hiermee bereiken we onder andere:

- Een goed geïmplementeerd privacybeleid, waarbij alle medewerkers zich ten volle bewust zijn van de noodzakelijkheid van een goede omgang met persoonsgegevens én van de ruimte die de wet- en regelgeving biedt om persoonsgegevens te verwerken.
- We passen de wettelijke eisen toe en gaan we respectvol om met de persoonsgegevens van burgers en met de persoonsgegevens van onze medewerkers.
- De rechten van betrokkenen worden gerespecteerd en zijn in onze procedures verankerd.
- Bij verwerking van persoonsgegevens worden alle relevante wettelijke grondslagen die verwerking mogelijk maken in de afweging betrokken en wordt gezocht naar de ruimte die de wet biedt.
- Afwijking van wet- en regelgeving vraagt om expliciete besluitvorming. Een besluit hiertoe moet gemotiveerd en met een risicoanalyse aan de Directieraad worden voorgelegd waarna besluitvorming door portefeuillehouder of college volgt. De FG wordt geïnformeerd.
- Het vertrouwen van burgers in de overheid wordt niet beschaamd.
- Het vertrouwen van onze medewerkers in de gemeente als werkgever wordt niet beschaamd.
- De risico's bij het verwijtbaar en onvoldoende beschermen van persoonsgegevens en het niet naleven van privacywet- en regelgeving worden zo veel mogelijk beperkt. Risico's zijn:
    - het betalen van schadevergoeding. Elke benadeelde heeft hier recht op;
    - reputatieschade en herstelkosten. Deze kunnen fors zijn en leiden tot verlies van vertrouwen in de overheid;
    - onderzoeken, dwangmaatregelen en hoge bestuurlijke boetes. Bij overtreding van de AVG kan de Autoriteit Persoonsgegevens (de landelijke toezichthouder, hierna AP) een boete opleggen. Onder de AVG kan de boete oplopen tot maximaal € 20.000.000.

Hiermee leggen we als gemeente de basis voor eenduidige aantoonbare naleving van de AVG. Daarnaast sluiten we aan bij de 3 centrale kernwaarden in de manier waarop de gemeente werkt: samenwerking (in – en extern), vertrouwen (integer, vriendelijk, eerlijk en open) en eigenaarschap ("we zijn ervan").

Naast dit door het college vastgestelde privacybeleid is informatiebeveiligingsbeleid vastgesteld. Hierin zijn maatregelen opgenomen om alle gegevens te beschermen. Informatiebeveiliging is een randvoorwaarde voor de borging van privacy bij de verwerking van persoonsgegevens.

1.3 Reikwijdte
Dit beleid is van toepassing van toepassing op:

- alle processen van de gemeente waarbinnen persoonsgegevens worden verwerkt (of die de gemeente uitbesteedt, inkoopt of op een andere manier organiseert);
- de onderliggende voorzieningen voor informatieverwerking en gegevensopslag (zowel papier als digitaal);
- alle ruimten en devices die door gemeenteambtenaren worden gebruikt waar(op) persoonsgegevens worden verwerkt,
- de gegevensuitwisseling met derden;
- de gehele levenscyclus van de verwerking van persoonsgegevens;
- de verwerking van statistische en/of geanonimiseerde gegevens, voor zover niet kan worden uitgesloten dat personen kunnen worden geïdentificeerd of geprofileerd.

2. Beleidsuitgangspunten

1. **Rechtmatige grondslag, behoorlijkheid en transparantie**
   Persoonsgegevens worden in overeenstemming met de wet- en regelgeving en op behoorlijke, zorgvuldige en transparante wijze verwerkt.

2. **Doelbinding**
   De gemeente zorgt ervoor dat persoonsgegevens alleen voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doelen worden verzameld en verwerkt. Persoonsgegevens worden alleen met een rechtmatige grondslag verwerkt.

3. **Dataminimalisatie (subsidiariteit en proportionaliteit)**
   De gemeente verwerkt alleen de persoonsgegevens die noodzakelijk zijn voor het vooraf bepaalde doel. De gemeente streeft naar minimale gegevensverwerking.

4. **Bewaartermijn**
   Persoonsgegevens worden niet langer bewaard dan nodig is. Het bewaren kan nodig zijn om de gemeentelijke taken goed uit te oefenen of om wettelijke verplichtingen na te leven.

5. **Beveiliging**
   Persoonsgegevens worden op passende wijze beveiligd. Dit is vastgelegd in het Informatiebeveiligingsbeleid Gemeente Eindhoven.

6. **Integriteit**
   Veilig omgaan met persoonsgegevens vereist een integere houding zoals ook van ambtenaren verwacht wordt.

7. **Delen met derden**.
   Bij samenwerking met externe partijen waarbij sprake is van verwerking van persoonsgegevens, maakt de gemeente afspraken over de eisen van gegevensuitwisseling en legt dit vast in overeenkomsten. In de relatie verwerkingsverantwoordelijke – verwerker wordt, vastgelegd op welke manier wordt voldaan aan de eisen die de AVG en de AP hieraan stelt. Indien er bij een verwerking sprake is van meerdere verwerkingsverantwoordelijken (gezamenlijk of individueel verwerkingsverantwoordelijk) wordt, naast een hoofdovereenkomst een gegevensuitwisselingsovereenkomst gesloten, waarin de zorgvuldige omgang met persoonsgegevens wordt geborgd.

8. **Functionaris gegevensbescherming (hierna FG)**
   De gemeentelijke FG voldoet aan de wettelijke eisen en heeft een onafhankelijke positie binnen de gemeente. De FG beschikt over voldoende faciliteiten om de informerende, adviserende en toezichthoudende taak uit te oefenen.

9. **Rechten van betrokkenen**
   De gemeente waarborgt de rechten van betrokkenen. Hiertoe zijn processen beschreven en ingericht.

10. **Ethiek en digitalisering**
    De gemeente heeft extra aandacht voor ethiek en digitalisering. Dit komt ook terug in het focusdocument “dataprotectie in de digitale samenleving” dat de AP voor de periode 2020 -2023 heeft opgesteld.

11. **Monitoren van burgers in de openbare ruimte**
    In het geval van verwerking van persoonsgegevens door het (digitaal) monitoren van burgers in de openbare ruimte vraagt dit expliciete bestuurlijke besluitvorming door het college vooraf aan de start van dergelijke verwerkingen.

12. **Uitvoering beleid**
    Het management stelt de benodigde mensen en (financiële) middelen beschikbaar zodat iedereen in staat is het privacybeleid in zijn/haar werkprocessen in te passen om een goede uitvoering van dit beleid te borgen.

13. **Actualisatie beleid**
    Het privacybeleid wordt in ieder geval iedere 4 jaar geëvalueerd aansluitend bij het focusdocument van de AP en indien nodig tussentijds gewijzigd

14. **Inwerkingtreding**
Dit privacybeleid treedt in werking na vaststelling en bekendmaking door het College van Burgemeester en Wethouders.

3. Toelichting

3.1 Algemeen AVG

De AVG regelt het algemene kader voor de omgang met persoonsgegevens in de Europese Unie. In Nederland zorgt de AP voor toezicht en handhaving van de Europese regels. De AVG is de hoogste wetgeving voor bescherming van persoonsgegevens en is de paraplu boven alle verwerkingen van persoonsgegevens door organisaties, zowel bedrijven als overheden. De uitgangspunten van de AVG zijn bijvoorbeeld:

- verwerking op rechtmatige, behoorlijke en transparante wijze (art 5 a);
- verzamelen voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden (art 5 b);
- verwerking alleen op een van de in de AVG opgenomen grondslagen (art 6).

Persoonsgegevens mogen alleen verwerkt worden voor een duidelijk omschreven doel (doelbinding). Op grond hiervan wordt de grondslag voor verwerking vastgesteld. De grondslagen zijn limitatief opgesomd in artikel 6 AVG. Dan wordt vastgesteld of de verwerkte gegevens proportioneel zijn (worden niet meer gegevens verwerkt dan noodzakelijk voor het uitoefenen van de taak?) en dat aan het subsidiariteitsbeginsel wordt voldaan (is er een voor de betrokkene minder belastende manier om de taak uit te voeren?). Persoonsgegevens, die door de gemeente worden verwerkt, moeten juist, actueel en volledig zijn.
De kernbeginselen van de AVG zijn dus transparantie, doelbinding, dataminimalisatie, kwaliteit/juistheid van gegevens en rechtmatige en behoorlijke verwerking.
Belangrijk is de 'accountability'. Dit houdt in dat een organisatie moet uitleggen en aantonen wat is gedaan om aan de regelgeving te voldoen. De AP heeft als externe toezichthouder een boetebevoegdheid van maximaal € 20 mln.
Voldoen aan accountability betekent niet alleen dat is voorzien in de invulling van de AVG, basisverplichtingen, zoals:

- een verwerkingenregister/documentatieplicht
- het treffen van passende technische en organisatorische maatregelen, waaronder juridische en beveiligingsmaatregelen;
- het opstellen van een procedure om beveiligingsincidenten en datalekken te melden en te documenteren (register datalekken), plus een procedure voor het melden van datalekken aan de AP;
- Data Protection Impact Analyse (hierna: DPIA) uitvoeren waar nodig;
- de verplichting tot aanstellen FG;
- de beschikking over goed stelsel van processen, werkafspraken en contracten waarin bescherming van persoonsgegevens is gewaarborgd,

maar ook dat duidelijk en transparant is hoe de open normen en begrippen van de AVG worden toegepast, welke keuzes worden gemaakt bij de uitvoering van de AVG en welke onderbouwing daarvoor wordt gegeven.

Daarnaast regelt de AVG het volgende:

- rechten van betrokkenen;
- het verwerken van bijzondere persoonsgegevens (art. 9 AVG) en het verder verwerken van reeds verzamelde gegevens (art. 6.4 AVG) is aan strikte voorwaarden gebonden.

Met externe partijen die in onze opdracht of in samenwerking persoonsgegevens verwerken, is een verwerkersovereenkomst verplicht. De externe partij is dan verwerker in de zin van de AVG. Met externe partijen die niet optreden als verwerker, maar als verwerkingsverantwoordelijke, worden alleen gegevens gewisseld indien daartoe een grondslag is, dit is opgenomen in het verwerkingsregister en nadat afspraken over een zorgvuldige omgang met persoonsgegevens zijn vastgelegd in een hoofdovereenkomst en een gegevensuitwisselingsovereenkomst.

3.2 Toelichting per beleidsuitgangspunt

3.2.1. Rechtmatige grondslag, behoorlijkheid en transparantie

Rechtmatige grondslag (artikel 6, AVG)
Rechtmatigheid, behoorlijkheid en transparantie zijn de centrale uitgangspunten vanuit de AVG. Een verwerking is rechtmatig, behoorlijk en transparant wanneer deze plaats vindt op basis van een zogenaamde grondslag. Deze zijn limitatief opgesomd in de wet te weten:

1. met toestemming van betrokkene voor de specifieke verwerking;
2. voor de uitvoering van een overeenkomst waarin betrokkene onderdeel was;
3. om een verplichting na te komen die in de wet staat;
4. vitale belangen (om ernstige bedreiging van betrokkene te bestrijden);
5. voor goede vervulling van een taak van algemeen belang of van een taak in het kader van de uitoefening van het openbaar gezag;
6. gerechtvaardigde belangen gemeente na belangenafweging.

De grondslagen voor verwerkingen voor de gemeente zijn met name de gronden genoemd onder 3 en 5. De laatste grondslag m.b.t. gerechtvaardigde belangen mag niet worden gebruikt voor de uitoefening van de gemeentelijk taak.

Register van verwerkingen (Artikel 30, AVG)
De gemeente moet een register aanleggen van alle verwerkingen waarvoor ze verantwoordelijk is. Het gaat dan om alle incidentele (bijvoorbeeld pilots) en structurele verwerkingen. Elk register bevat een beschrijving van wat tijdens een verwerking plaatsvindt en welke gegevens worden gebruikt, namelijk:

- naam en contactgegevens van de verwerkingsverantwoordelijke en, mogelijk, de verwerker(s) en andere verwerkingsverantwoordelijke(n);
- doelen van de verwerking;
- beschrijving van persoonsgegevens en bijbehorende betrokkenen;
- beschrijving van de ontvangers van de persoonsgegevens;
- beschrijving van het verstrekken van persoonsgegevens aan een derde land of internationale organisatie;
- termijnen waarin persoonsgegevens moeten worden gewist;
- algemene beschrijving van de beveiligingsmaatregelen.

Het is aan de verwerkingsverantwoordelijke om ervoor te zorgen dat het register altijd actueel en volledig is. Ook de inhoud van het verwerkingsregister valt onder de verantwoordelijkheid van de verwerkingsverantwoordelijke.
Binnen deze kaders wordt het verwerkingsregister van de gemeente centraal bij de FG beheerd.

Data Protection Impact Assessment, DPIA (Artikel 35, AVG)
Een DPIA ofwel gegevensbeschermingseffectbeoordeling beoordeelt de effecten en risico's van nieuwe, gewijzigde of bestaande verwerkingen op de bescherming van persoonsgegevens. Een DPIA is verplicht bij een risicovolle verwerking. De gemeente voert deze uit als er sprake is van een verwerking die voldoet aan de criteria van een risicovolle verwerking, zoals een geautomatiseerde verwerking, een grootschalige verwerking of een grootschalige monitoring van openbare ruimten. Dit geldt in het bijzonder bij nieuwe technologieën.
Voor alle verwerkingen wordt advies gevraagd aan de FG over het uitvoeren van een DPIA. Niet alleen op voorhand, maar ook over het uitvoeren van een DPIA alsmede over de uit de DPIA voortgekomen maatregelen.
Een DPIA wordt tijdig uitgevoerd. Dit betekent in ieder geval voordat de verwerking start of voordat de wijziging van een verwerking operationeel wordt. De uit de DPIA voortvloeiende maatregelen om risico's te minimaliseren worden tijdig geïmplementeerd. Dat wil zeggen voordat de verwerking start of voordat een wijziging van een verwerking operationeel wordt.

Informatieplicht (Artikel 13,14, AVG)
De gemeente informeert betrokkenen over het verwerken van persoonsgegevens op of voor het moment dat betrokkene ze beschikbaar stelt. Worden de gegevens buiten de betrokkene om verkregen, informeren we de betrokkene op het moment dat ze voor de eerste keer worden verwerkt. Tenzij er een grond is om achteraf te informeren.

3.2.2. Doelbinding

Volgens artikel 5 AVG mogen persoonsgegevens alleen verzameld worden als een doel is vastgesteld. Dit moet uitdrukkelijk omschreven en gerechtvaardigd zijn. Gegevens mogen nooit voor andere doelen verwerkt worden. Voor de uitvoering van wetten zoals de Jeugdwet zijn de doelen al in de wet vastgelegd, net als de persoonsgegevens die gevraagd en verwerkt mogen worden. Bij verzameling of gebruik van grote aantallen gegevens (open/big data) vraagt de doelbinding extra aandacht als er verwerking van persoonsgegeven plaatsvindt. De AVG staat profilering in principe niet toe.

3.2.3. Dataminimalisatie (subsidiariteit en proportionaliteit)
Waar mogelijk worden minder of geen persoonsgegevens verwerkt. We beperken inbreuk op de persoonlijke levenssfeer van de betrokkene zoveel mogelijk en zoeken altijd de minst belastende manier. Inbreuk op de belangen van de betrokkene mag niet onevenredig zijn in verhouding tot het doel. Hoofdregel is dat het alleen toegestaan is in overeenstemming met de wet en op een zorgvuldige wijze.

Persoonsgegevens worden zoveel mogelijk verzameld bij de betrokkene zelf. De wet gaat uit van subsidiariteit: verwerking is alleen toegestaan als het doel niet op een andere manier kan worden bereikt. In de wet wordt ook gesproken over proportionaliteit: gegevens mogen alleen worden verwerkt als dit in verhouding staat tot het doel. Kunnen we zonder of met minder (belastende) persoonsgegevens hetzelfde doel bereiken, kiezen we daar altijd voor. De gemeente zorgt dat de gegevens actueel, juist en volledig zijn.

3.2.4. **Bewaartermijn**

Het bewaren kan nodig zijn om de gemeentelijke taken goed uit te oefenen of om wettelijke verplichtingen na te leven. De gemeente bewaart de persoonsgegevens niet langer dan nodig voor het doel van de verwerking. M.a.w. persoonsgegevens worden niet langer bewaard dan nodig is. Dit houdt in dat deze gegevens vernietigd worden of zó worden aangepast dat de informatie niet meer gebruikt kan worden om iemand te identificeren. Een vastgestelde bewaartermijn moet in het kader van transparantie voor zover mogelijk gemeld worden aan de betrokkenen.
De AVG geeft geen concrete bewaartermijn voor persoonsgegevens. Wel staat in de wet dat een persoonsgegeven alleen mag worden bewaard als identificeerbaar gegeven, voor zolang het nodig is voor de doeleinden waarvoor het verzameld is (opslagbeperking). Het is mogelijk om gegevens langer te bewaren als deze geanonimiseerd worden, zodat directe of indirecte identificatie van een persoon niet meer mogelijk is. Er zijn uitzonderingen voor archivering, algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden. Bij de verwerking wordt vastgelegd welke bewaartermijn wordt gehanteerd. Er moet binnen elk gegevensverwerkend proces gezocht worden naar de minimale set van gegevens die voor de kortst mogelijke tijd wordt bewaard. Vragen ter bepaling van de bewaartermijn zijn:

- Wanneer is het procesdoel behaald?
- Kan ik gegevens gedurende de bewaartermijn actueel, juist en volledig houden?
- Kunnen als het doel is behaald de gegevens worden vernietigd zonder afbreuk te doen aan het proces?
- Is het langer bewaren van de gegevens een grotere inbreuk op de persoonlijke levenssfeer van de betrokkenen?
- Zijn de risico's op ongewenste verspreiding ook bij langer bewaren klein (de kans wordt tenslotte groter als er meer tijd is)?
- Is er een wettelijke plicht de gegevens te bewaren?
- Kunnen de gegevens ook geanonimiseerd worden?
- Kan ik een betrokkene tijdens de hele bewaartermijn toegang tot de gegevens geven?

In het kader van accountability is "het zou weleens handig zijn voor ons" geen reden.
E.e.a. staat los van hetgeen in de Archiefwet is bepaald. Doelstelling van de Archiefwet is zorgdragen voor het permanent bewaren van geselecteerde informatie ten behoeve van geheugen en kennisbehoud aan de hand van vooraf vastgestelde selectiecriteria.

3.2.5. **Beveiliging**

Persoonsgegevens worden op passende wijze beveiligd. Dit is vastgelegd in het Informatiebeveiligingsbeleid Gemeente Eindhoven en eventueel in een aanvullend beveiligingsplan specifiek opgesteld voor een proces of registratie.
De gemeente beveiligt alle persoonsgegevens zodat gegevens niet worden ingezien of gewijzigd door iemand die daar geen recht toe heeft. Indien dit wel gebeurt spreken we van een datalek. Dan is er inbreuk op beveiliging van persoonsgegevens. Bv. als onbedoeld toegang wordt geboden tot persoonsgegevens of als er sprake is van verlies, wijziging of vrijkomen van persoonsgegevens bij een organisatie. Niet alleen het vrijkomen of lekken van gegevens is een datalek, ook als onrechtmatig gegevens worden verwerkt, is hiervan sprake. Voor het afhandelen van datalekken is een procedure vastgesteld. De gemeente heeft een registratieplicht. Dit houdt in dat meldingen van (mogelijke) datalekken, worden bijgehouden in een register. Hierin zijn de details van de datalekken vastgelegd. Ieder (mogelijk) datalek wordt door de verwerkersverantwoordelijke doorgegeven aan bureau FG, door bureau FG beoordeeld en vervolgens door bureau FG opgenomen in het datalekkenregister van de gemeente. De verwerkingsverantwoordelijke sectoren zijn verantwoordelijk voor de inhoud van dit register en voor het tijdig aanleveren van de correcte en volledige informatie ten behoeve van dit register. Ook is het aan de verwerkingsverantwoordelijke sector om betrokkenen te informeren over een datalek. Als een datalek ernstige nadelige gevolgen kan hebben voor de persoonlijke levenssfeer van betrokkenen moet het datalek binnen 72 uur na ontdekking van het datalek worden gemeld bij de AP . Dit wordt de meldplicht van datalekken genoemd. Bureau FG meldt dergelijke datalekken bij de AP. De verwerkersverantwoordelijke sector levert daartoe tijdig alle noodzakelijke informatie aan.

3.2.6. **Integriteit**

Iedere (nieuwe) medewerker wordt door de verwerkersverantwoordelijke aantoonbaar geïnformeerd over het zorgvuldig omgaan met persoonsgegevens, bijvoorbeeld via instructies. Daarnaast legt iedere ambtenaar een ambtseed af. Integriteit, zoals verwoord in de Gedragscode Ambtenaren 2020, is hiervan een onderdeel.

3.2.7. Delen met derden

Met derden die in onze opdracht of in samenwerking persoonsgegevens verwerken, is een verwerkersovereenkomst verplicht. De derde is dan verwerker in de zin van de AVG. Bij samenwerking met derden waarbij sprake is van verwerking van persoonsgegevens, maakt de gemeente/sector afspraken over de eisen van gegevensuitwisseling en legt dit vast in overeenkomsten. In de relatie verwerkingsverantwoordelijke – verwerker wordt vastgelegd op welke manier wordt voldaan aan de eisen die de AVG en de AP hieraan stelt. Indien er bij een verwerking sprake is van meerdere verwerkingsverantwoordelijken (gezamenlijk of individueel verwerkingsverantwoordelijk) wordt, naast een hoofdovereenkomst een gegevensuitwisselingsovereenkomst gesloten. Hiervoor hanteren wij een standaard verwerkersovereenkomst. Hierin staan in ieder geval de volgende afspraken:

- omschrijving van onderwerp, duur, aard en doel van de verwerking, het soort persoonsgegevens, de categorieën van betrokkenen en rechten en verplichtingen van de gemeente als verwerkingsverantwoordelijke.
- verwerking vindt uitsluitend plaats op basis van onze schriftelijke instructies. Verwerker mag de persoonsgegevens niet voor andere of eigen doeleinden gebruiken.
- Personen in dienst van of werkzaam voor de verwerker hebben geheimhoudingsplicht.
- Verwerker treft passende technische en organisatorische maatregelen om de verwerking te beveiligen. Bijvoorbeeld pseudonimisering en versleuteling van persoonsgegevens, permanente informatiebeveiliging, herstel van beschikbaarheid en toegang tot gegevens bij incidenten, regelmatige beveiligingstesten.
- Verwerker schakelt geen subverwerker(s) in zonder onze voorafgaande schriftelijke toestemming. Verwerker legt aan de subverwerker in een subverwerkersovereenkomst dezelfde verplichtingen op als de verwerker richting de gemeente heeft. In de verwerkersovereenkomst direct afgesproken zijn dat, en onder welke voorwaarden, de verwerker subverwerkers mag inschakelen. Komt de subverwerker de verplichtingen niet na, dan blijft verwerker volledig aansprakelijk jegens ons voor het nakomen van de verplichtingen van de subverwerker (zie artikel 28, lid 4 van de AVG).
- Verwerker helpt om te voldoen aan onze plichten als betrokkenen hun privacy rechten uitoefenen (zoals het recht op inzage, correctie en vergetelheid).
- Verwerker helpt ook andere verplichtingen na te komen, zoals bij het melden van datalekken, het uitvoeren van een data protection impact assessment (DPIA) en een voorafgaande raadpleging.
- Na afloop van de verwerkingsdiensten verwijdert de verwerker de gegevens én kopieën of bezorgt deze op verzoek aan ons terug. Tenzij de verwerker wettelijk verplicht is de gegevens te bewaren.
- Verwerker werkt mee aan onze audits of die van een derde partij en stelt alle relevante informatie beschikbaar om te controleren of hij zich houdt aan de hierboven genoemde verplichtingen (uit artikel 28 AVG).

3.2.8. Functionaris gegevensbescherming (FG)

De gemeente heeft een FG aangesteld. De gemeentelijke FG voldoet aan de wettelijke eisen en heeft een onafhankelijke positie binnen de gemeente. De FG heeft een informerende, adviserende en toezichthoudende taak. De adviezen van de FG worden als zwaarwegend aangemerkt. Dit laatste is uiteraard het uitgangspunt. Afwijking van een FG advies vindt gemotiveerd plaats. Uiteraard wordt de FG geïnformeerd over deze afwijking van het advies.

De FG beschikt over voldoende faciliteiten om de informerende, adviserende en toezichthoudende taak uit te oefenen. De taken van de FG zijn als volgt:

- Wettelijke taken (artikel 39 AVG):
  - Informeren en adviseren van de verwerkingsverantwoordelijken over hun verplichtingen uit hoofde van de AVG;
  - Toezien op naleving van de AVG door de verwerkingsverantwoordelijken of door hen ingeschakelde verwerkers;
  - Advisering over de uitvoering van DPIA's en toezien op de uitvoering daarvan;
  - Samenwerken met de AP en optreden als contactpunt voor de AP.

- Overige taken:
  - bevorderen dat risico's, van verwerken van persoonsgegevens binnen de gemeente, zoveel als mogelijk worden beperkt;
  - de verantwoordelijken en collega's zowel gevraagd als ongevraagd te adviseren toepassing van wet- en regelgeving met betrekking tot de verwerking van persoonsgegevens;

- stimuleren dat de gemeente Eindhoven privacy vriendelijke systemen en processen toepast en privacy risico's worden geminimaliseerd;
- het bewaken van de naleving van de regels door onafhankelijk onderzoek te doen naar het (mogelijke) niet naleven ervan.
- rapporteren aan gemeentesecretaris en bestuur;
- toezien dat privacy rechten van burgers worden nageleefd;
- optreden als "ombudsman" voor burgers en medewerkers bij klachten over de wijze waarop de organisatie met hun persoonsgegevens is omgegaan;
- samenwerken met FG's van andere gemeenten of bedrijven;
- zich sterk maken voor een actueel en volledig centraal register van verwerkingen;
- beoordelen van doorgegeven datalekken, het opnemen van deze datalekken in een centraal register en het melden van datalekken bij de AP.
- stimuleren van een lerende organisatie naar aanleiding van datalekken;
- houdt een overzicht bij van afgeronde en lopende DPIA's.
- draagt bij aan de privacy awareness van de organisatie.

De FG heeft recht op toegang tot alle informatie, systemen en processen waarin bescherming van persoonsgegevens een rol speelt of zou kunnen spelen. De FG geniet ontslagbescherming en werkt vrij van last en opdracht. De FG brengt rechtstreeks verslag uit aan de gemeentesecretaris en aan de burgemeester c.q. het college van burgemeester en wethouders.

De verwerkingsverantwoordelijke sectoren zorgen ervoor dat de FG naar behoren en tijdig wordt betrokken bij alle aangelegenheden die verband houden met de bescherming van persoonsgegevens.

3.2.9. Rechten van betrokkenen
De wet bepaalt niet alleen de plichten van degenen die de persoonsgegevens verwerken, maar ook de rechten van de personen van wie de gegevens worden verwerkt. Deze rechten worden ook wel de rechten van betrokkenen genoemd en bestaan uit:

- recht op informatie (artikelen 13 en 14): betrokkenen hebben het recht om aan de gemeente te vragen of zijn/haar persoonsgegevens worden verwerkt.
- inzagerecht (artikel 15): betrokkenen hebben de mogelijkheid om te controleren of, en op welke manier, zijn/haar gegevens worden verwerkt.
- correctierecht (artikel 16): als gegevens duidelijk niet kloppen, kan betrokkene een verzoek indienen bij de gemeente om dit te corrigeren.
- recht om vergeten te worden/recht op vergetelheid (artikel 17): heeft betrokkene toestemming gegeven om gegevens te verwerken, heeft betrokkene het recht om die gegevens te laten verwijderen. Bijvoorbeeld ook als de verwerking onrechtmatig gebeurt.
- recht op beperking van verwerking (artikel 18): in bepaalde situaties hebben betrokkenen er recht op dat hun persoonsgegevens (tijdelijk) niet gebruikt worden
- recht op overdraagbaarheid/ dataportabiliteit (artikel 20): dit recht houdt in dat een betrokkene de gegevens van een verwerkingsverantwoordelijke moet kunnen verkrijgen in gestructureerde, gangbare en machine leesbare vorm en het recht heeft deze gegevens aan een andere verwerkingsverantwoordelijke over te dragen of rechtstreeks te laten overdragen, zonder daarbij te worden gehinderd tenzij dit afbreuk doet aan rechten en vrijheden van anderen. Een betrokkene heeft recht op overdraagbaarheid voor zover het gaat om door hem zelf verstrekte gegevens.
- recht van bezwaar (artikel 21): betrokkenen hebben het recht aan de gemeente te vragen om hun persoonsgegevens niet meer te gebruiken.
- recht op een menselijke blik bij besluiten/non profiling (artikel 22) : als op basis van automatisch verwerkte gegevens een besluit over iemand is genomen, kan iemand een nieuw besluit verlangen waar de gegevens door een mens worden beoordeeld.

Indienen van verzoek
Om gebruik te maken van zijn/haar rechten kan de betrokkene een verzoek indienen bij de verwerkingsverantwoordelijke. De gemeente heeft vanaf ontvangst van het verzoek vier weken de tijd om een besluit te nemen op het verzoek. Wordt deze termijn overschreden, dan kan betrokkene de gemeente in gebreke stellen of een klacht indienen bij de FG. Voordat een verzoek in behandeling kan worden genomen, dient de identiteit van betrokkene vastgesteld te worden. Dit om fraude te voorkomen.
De gemeente voldoet aan het verzoek, tenzij er gerechtvaardigde gronden zijn om een verzoek af te wijzen. Een betrokkene heeft het recht om bezwaar te maken tegen de beslissing.

3.2.10. Ethiek en digitalisering.
De gemeente heeft extra aandacht voor ethiek en digitalisering. Dit komt ook terug in het focusdocument "dataprotectie in de digitale samenleving" van de AP. Hierin geeft de AP aan dat de risico's van de di-

gitaliserende samenleving voor de bescherming van persoonsgegevens groot, divers en complex zijn. Het gaat om:

1. Datahandel. Dit ziet met name op ongeoorloofde doorgifte of doorverkoop van data/ persoonsgegevens.
2. Digitale overheid. Welke keuzes maakt de overheid bij het inzetten van persoonsgegevens en zijn de keuzes verantwoord:
    - databeveiliging; De AP verwacht van de overheid dat structureel wordt geïnvesteerd in informatiebeveiliging. IT systemen moeten worden ge-audit als onderdeel van data boekhouding.
    - Smart City projecten: De aanwezigheid van sensoren in de stad heeft risico's. De AP wil dat zo min mogelijk data/persoonsgegevens wordt verzameld conform AVG.
    - ongeoorloofd delen; het delen/koppelen van bestanden kan een schending zijn van het wettelijke beginsel van doelbinding. De overheid moet terughoudend zijn met het delen van bestanden.
    - verkiezingen en micro targeting; politieke partijen moeten de AVG naleven. De AP zal hierop actief toezicht houden.

3. Artificiële intelligentie (hierna AI) en algoritmes. De inzet van AI en algoritmes biedt voordelen, maar ook risico's en schadelijke effecten. Hoe wordt daar mee omgegaan? Dit zijn onderwerpen met een groot risico voor bewoners. De AP legt hier de komende jaren extra nadruk op bij haar toezicht.

Vanzelfsprekend wordt door de gemeente rekening gehouden met deze focusgebieden bij de uitvoering van de AVG en daarmee is voor de periode 2020-2023 aandacht voor de onderwerpen zoals door de AP geformuleerd in haar visiedocument 'dataprotectie in de digitale samenleving'.

3.2.11 Actualisatie beleid

Het privacybeleid wordt in ieder geval iedere 4 jaar geëvalueerd aansluitend bij het focusdocument van de AP en indien nodig tussentijds gewijzigd. Dit doen we door de verschillende stakeholders zoals ook opgenomen op de pagina's 20 en 21 van dit beleid vanuit ieders invalshoek input te geven op het beleid. Vanuit de CPO wordt dit aangestuurd. Dit staat los van de periodieke herzien van de jaarplannen die onder dit beleid hangen en voorzien in de jaarlijkse ute qua operationele uitvoeringstaken.

4. AVG compliance

De facto zorgt de AVG er voor dat compliance op het gebied van bescherming van persoonsgegevens voor de gemeente als gegevensverwerkende organisatie een niet vrijblijvende verplichting is.

De gemeente is verantwoordelijk voor het aantoonbaar naleven van de AVG bij de verwerking van persoonsgegevens. Artikel 24 lid 1 AVG bepaalt dat de gemeente als verwerkingsverantwoordelijke passende technische en organisatorische maatregelen moet treffen om te waarborgen en te kunnen aantonen dat verwerkingen in overeenstemming met de AVG worden uitgevoerd. Deze maatregelen moeten worden geëvalueerd en indien nodig geactualiseerd.
De gemeente voorziet in deze verplichting door middel van het richten, inrichten en verrichten van onderhavig privacybeleid door het verstrekken van informatie (het berichten over het waarom, de voortgang en de resultaten).
Het expliciet beleggen van verantwoordelijkheden en bijbehorende activiteiten, procedures en instrumenten, zorgt voor het daadwerkelijk en structureel uitvoeren en borgen van de beheersmaatregelen.
Compliance is een continue ontwikkelproces:

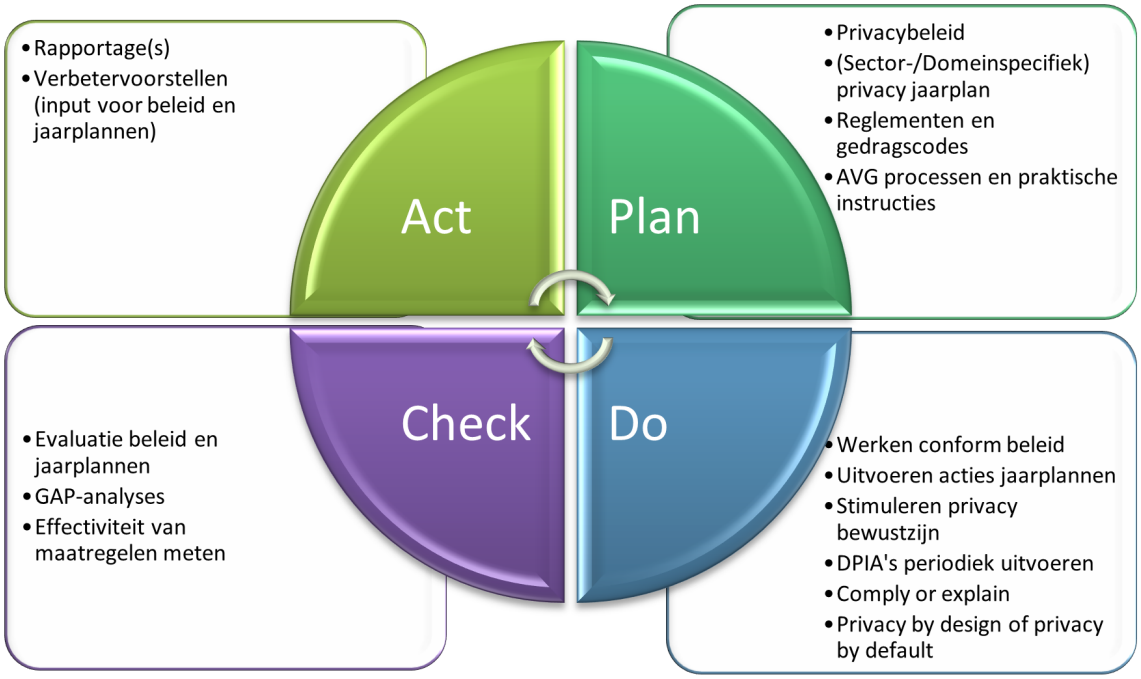
AVG compliance is in belang van de gemeentelijke organisatie en van degenen wiens gegevens verwerkt worden. Gebeurt dit niet, dan kan dat consequenties hebben:

- Op overtreding staat een maximale boete van 20 miljoen euro, uit te delen door de AP.
- Naast administratieve geldboetes is de AP bevoegd een verwerkingsverantwoordelijke corrigerende maatregel op te leggen. Denk aan de verplichting te stoppen met een bepaalde gegevensverwerking of aan de eis een betrokkene alsnog in kennis te stellen van een datalek.
- Een burger die, of een bedrijf dat, schade lijdt doordat de AVG niet is nageleefd, kan een schadevergoeding eisen.
- Reputatieschade wanneer bekend wordt dat in strijd met de AVG is gehandeld.

4.1 AVG beheer cyclus

Voldoen aan de compliance verplichting vereist het actueel houden hiervan via een PDCA (Plan-Do-Check-Act) cyclus en een positieve en actieve betrokkenheid *iedereen*. Hierdoor wordt de kans op het maken van fouten in de verwerking van persoonsgegevens en de kans op datalekken verkleind.

De PDCA-cyclus vormt het managementsysteem van privacy om compliance blijvend te beheersen en waarbij elke verbeterstap wordt geborgd:



4 .2 AVG processen

Uitgangspunt is dat AVG-compliance aangetoond wordt vanuit de procesarchitectuur van de gemeente (dus niet vanuit systemen, techniek, e.d.). De procesarchitectuur is namelijk de verbindende factor tussen de medewerkers, processen, applicaties, data (waaronder persoonsgegevens) en infrastructuur.

De volgende AVG-processen zijn gemeente breed ingericht:

- Beheren verwerkingenregister: een register bijhouden van alle verwerkingen waarvoor de gemeente verantwoordelijk is (artikel 30 AVG). Elk verwerking bevat o.a. de grondslag, een beschrijving van wat tijdens een verwerking plaatsvindt, welke gegevens worden verwerkt, naam en contactgegevens van de verwerkingsverantwoordelijke (en evt. verwerkers en andere verwerkingsverantwoordelijken), doelen van de verwerking, bewaartermijnen, algemene beschrijving van de beveiligingsmaatregelen. Het is aan de verwerkingsverantwoordelijke sector om ervoor te zorgen dat het register altijd actueel en volledig is.
- Uitvoeren Data Protection Impact Assessment (DPIA): een gegevensbeschermingseffectbeoordeling uitvoeren om de effecten en risico's van nieuwe, gewijzigde of bestaande verwerkingen van persoonsgegevens te beoordelen (artikel 35 AVG). Een DPIA is verplicht bij een risicovolle verwerking (zoals een geautomatiseerde verwerking, een grootschalige verwerking of een grootschalige monitoring van openbare ruimten, bij nieuwe technologieën, etc.). De Functionaris Gegevensbescherming adviseert voorafgaand aan een DPIA én aan het einde over de maatregelen. Een DPIA wordt uitgevoerd voordat de verwerking start of voordat de wijziging van een verwerking operationeel wordt. Ook worden de uit de DPIA voortvloeiende maatregelen om risico's te minimaliseren geïmplementeerd voordat de verwerking start of voordat een wijziging van een verwerking operationeel wordt. Met andere woorden: een DPIA is afgerond wanneer de beheersmaatregelen geïmplementeerd zijn.
- Uitvoeren rechten van betrokkenen (artikel 13 t/m 17 AVG). Recht op inzage is het recht van mensen om onder meer een kopie te ontvangen van de persoonsgegevens die u van hen verwerkt. Recht op vergetelheid is het recht om vergeten te worden. Recht op rectificatie en aanvulling is het recht om de persoonsgegevens die u verwerkt te laten wijzigen. Het recht op dataportabiliteit is het recht om persoonsgegevens over te laten dragen aan een andere partij. Het recht op beperking van de verwerking is recht om minder gegevens te laten verwerken. Het recht met betrekking tot geautomatiseerde besluitvorming en profilering is het recht op een menselijke blik bij besluiten. Het recht om bezwaar te maken tegen de gegevensverwerking.
- Afsluiten en beheren verwerkersovereenkomsten.

- Uitvoeren registratie en meldplicht datalekken.

Voor de processen geldt dat alle verwerkersverantwoordelijke sectoren verantwoordelijk zijn voor de uitvoering hiervan. In concreto zijn de 14 sectorhoofden dus verantwoordelijk proceseigenaar van de AVG-processen.

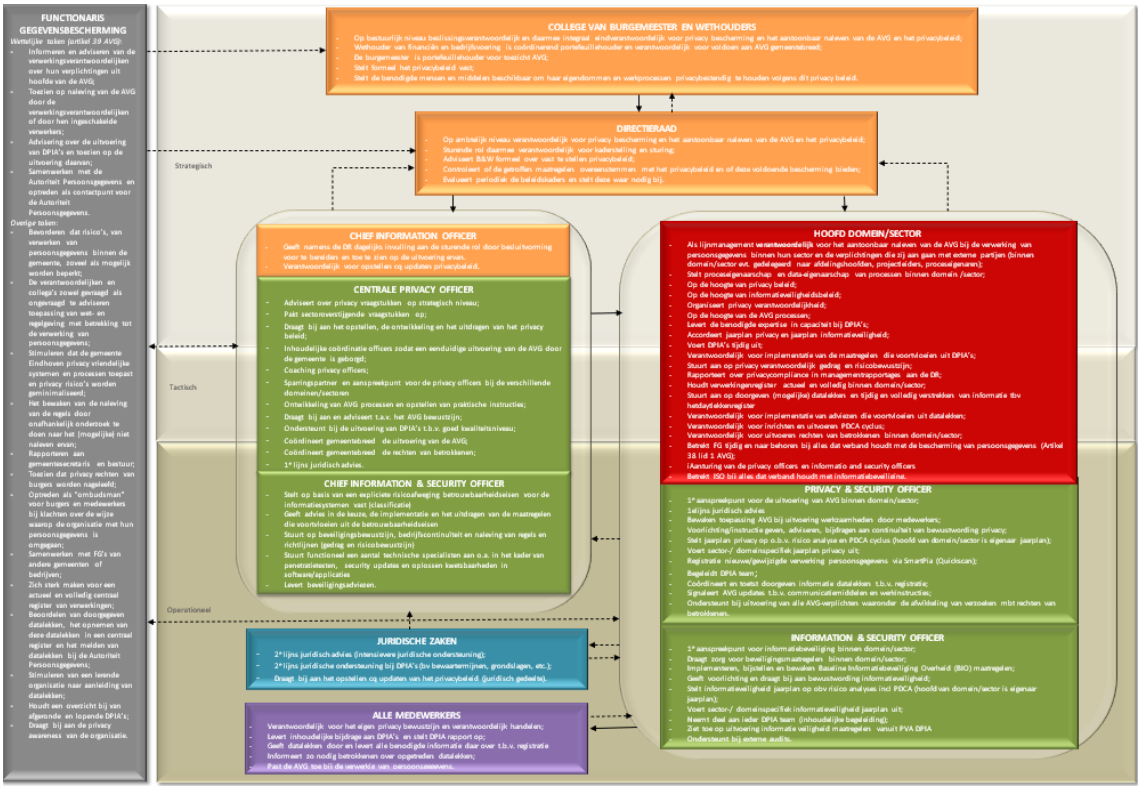
4 .3 AVG governance

De bescherming van persoonsgegevens is een inherent onderdeel van ieders functie c.q. ieders dagelijks handelen. Tegelijkertijd is de bescherming van persoonsgegevens niet de core business van de meeste medewerkers. Er zijn daarom medewerkers aangewezen om hen daarbij te ondersteunen en om als vraagbaak te fungeren.
De sectorhoofden zijn op ambtelijk niveau verwerkingsverantwoordelijk voor de aantoonbare naleving van de AVG en de uitgangspunten van het privacybeleid binnen de eigen sector. Zij moeten:
kunnen aantonen dat naleving plaats vindt en op welke wijze;
de Centrale Privacy & Security Officer, de Privacy & Security Officers, de Chief Information Security Officer en de Information Security Officers in staat stellen medewerkers bij te staan bij het uitvoeren van de AVG en dit privacybeleid.
De verantwoordelijkheden t.a.v. de aantoonbare naleving van de AVG beginselen en de uitgangspunten van het privacybeleid zijn aan de hand van het RASCI-model vastgesteld:

	R	A	S	C	I
College van burgemeester en wethouders		✓			✓
Directieraad	✓				✓
Sectorhoofden (op sectorniveau)	✓	✓			✓
Afdelingshoofden / projectleiders	✓				✓
Proceseigenaren	✓				✓
Chief Information Officer	✓				✓
Centrale Privacy Officer (sectoroverstijgend)			✓	✓	✓
Privacy Officer (op sectorniveau)			✓	✓	✓
Chief Information & Security Officer (sectoroverstijgend)				✓	✓
Information & Security Officer (op sectorniveau)			✓	✓	✓
Alle medewerkers (incl. inhuur en externen)			✓		✓
Juridische zaken			✓	✓	
Functionaris Gegevensbescherming				✓	✓
Gemeenteraad					✓
Belanghebbenden/betrokkenen					✓
Autoriteit Persoonsgegevens					✓

Uitleg RASCI:
R = Responsable (feitelijk verantwoordelijk)
A = Accountable (eindverantwoordelijk)
S = Supporting (ondersteunend, uitvoerend)
C = Consulted (adviserend, controlerend)
I = Informed (geïnformeerd)

Op de volgende pagina is expliciet de interne organisatie aangegeven met taken, rollen, verantwoordelijkheden en bevoegdheden op strategisch, tactisch en operationeel niveau (= "AVG-organisatieplaat gemeente Eindhoven"). Hier komen governance en PDCA samen.



Eindhoven, .
Het college van burgemeester en wethouders van Eindhoven,
,burgemeester
, secretaris
Mij bekend,
De gemeentesecretaris van Eindhoven