PURMEREND

GEMEENTEBLAD

Officiële uitgave van de gemeente Purmerend

Nr. 107466

23 mei

2018

PRIVACYBELEID GEMEENTE PURMEREND

INHOUDSOPGAVE

INLEIDING

Privacy is een grondrecht. Artikel 10 van de Grondwet verwoordt het als volgt:
Ieder heeft, behoudens bij of krachtens de wet te stellen beperkingen, recht op eerbiediging van zijn persoonlijke levenssfeer.
Privacy is o.a. bescherming van je lichamelijke integriteit, is inachtneming van je huisrecht.
Privacy is ook bescherming van de gegevens die iets over jou als mens zeggen; bescherming van persoonsgegevens dus. Over dit laatste aspect van privacy gaat dit beleid.

De bescherming van persoonsgegevens staat momenteel in het middelpunt van de belangstelling.
Waarom?
Omdat op 25 mei 2018 de Europese Algemene verordening gegevensbescherming (AVG) in werking treedt.
Omdat niemand er aan ontkomt dat zijn persoonsgegevens – dagelijks – worden verwerkt.
Omdat de mogelijkheden om persoonsgegevens te verwerken en te delen met de toename van de technologische ontwikkelingen steeds groter worden.
Omdat sinds de inwerkingtreding van de Wet meldplicht datalekken is aangetoond dat het regelmatig mis gaat en de bescherming van persoonsgegevens tóch niet optimaal bleek te zijn.
Omdat… nou gewoon: omdat het belangrijk is dat burgers erop kunnen vertrouwen dat iedereen die bij de gemeente Purmerend persoonsgegevens over hen verwerkt daarover nadenkt, daarover transparant is en de bescherming daarvan hoog in het vaandel heeft staan.

DAAROM dus een privacybeleid waarin wordt aangegeven hoe de verwerkings-verantwoordelijken van de gemeente Purmerend invulling geven aan hun verplichtingen op grond van (met name) de AVG. Als gemeente staan we voor de inwoners van de stad. We realiseren ons dat een al te stringent privacykader ons werk voor de Purmerenders lastiger kan maken. Denk maar aan inwoners die meerdere keren dezelfde gegevens in verschillende aanvraagformulieren moeten invoeren. Dat is niet altijd handig. Ook kan het erg aantrekkelijk zijn om voor de uitvoering van onze taken (en om de inwoners beter van dienst te zijn) gegevens te combineren of te delen met andere collega's of zelfs externe instanties.

Het privacybelang wegen wij af tegen en naast de andere belangen die wij als (verwerkingsverantwoordelijken van de) gemeente voor de inwoners dienen.

Als basis geldt dat we de privacyregels zoals we die in dit beleid opnemen in acht nemen. Daar waar het onevenredige belemmeringen vormt voor de uitvoering van onze taken, durven we die ter discussie te stellen. Als dat aan de orde is, proberen we de betrokkenen zo goed mogelijk daarover te informeren en gaan daarover in gesprek met de Autoriteit Persoonsgegevens (AP).

REIKWIJDTE GEMEENTELIJK PRIVACYBELEID

1. Domeinoverstijgend
Dit privacybeleid bevat de domeinoverstijgende richtlijnen over hoe de bescherming van persoonsgegevens binnen de gemeentelijke organisatie wordt vormgegeven en georganiseerd.
Waar nodig, kunnen voor een specifiek domein of een specifiek team aanvullende regels worden gesteld.

2. Verwerkingsverantwoordelijke overstijgend
Dit privacybeleid is een gezamenlijk product van alle verwerkingsverantwoordelijken van de gemeente Purmerend. Het is daarom van toepassing op alle verwerkingen van persoonsgegevens binnen de gemeentelijke organisatie, ongeacht onder wiens verantwoordelijkheid ze plaatsvinden.

3. Ambtenaar overstijgend
Dit privacybeleid richt zich op een ieder die binnen de gemeentelijke organisatie persoonsgegevens verwerkt. Het maakt daarbij niet uit of iemand zelf bestuurder c.q verwerkingsverantwoordelijke is, medewerker in (al dan niet vaste) dienst is of krachtens een (tijdelijke) overeenkomst werkzaamheden verricht.
NB: met verwerkers worden aparte afspraken gemaakt. Op hen is dit privacybeleid daarom niet van toepassing.

4. Wet overstijgend
Onder andere de volgende wetten bevatten bepalingen over de verwerking van persoonsgegevens: de Wet bescherming persoonsgegevens (Wbp), per 25 mei 2018: de (uitvoeringswet) AVG, de Wet basisregistratie personen, Wmo 2015, Jeugdwet en Wabo.
Voor de toepasselijkheid van dit beleid maakt het niet uit op basis van welke van deze wetten de verwerking van persoonsgegevens plaatsvindt.

5. Device en systeem overstijgend
De verwerking van persoonsgegevens kan geautomatiseerd plaatsvinden of handmatig. Gegevens kunnen verwerkt worden via een desktop, een laptop, tablet of een smartphone.
Het privacybeleid is van toepassing op alle verwerkingen van persoonsgegevens door/binnen de gemeentelijke organisatie, ongeacht hoe of waarop deze plaatsvindt.

6. Verhouding met Informatiebeveiliging(sbeleid)
De Wbp en de AVG eisen een passende beveiliging van persoonsgegevens. Ook andere gegevens moeten echter goed beveiligd worden; denk aan bedrijfsgegevens die een rechtspersoon vertrouwelijk aan de gemeente geeft in het kader van een af te sluiten overeenkomst. Denk ook aan de eigen financiële gegevens vóórdat ze via de begroting aan de gemeenteraad worden verstrekt.
Er is daarom een apart gemeentelijk informatiebeveiligingsbeleid (IB-beleid) dat ziet op de beveiliging van alle gegevens, of het nu persoonsgegevens zijn of niet. Dit beleid en het onderhavige privacybeleid vullen elkaar aan.

BEGRIPSBEPALINGEN

In dit privacybeleid worden begrippen gehanteerd die uitleg behoeven. Voor niet omschreven begrippen, wordt verwezen naar de definities in artikel 4 van de AVG.

- Persoonsgegevens: alle informatie over een direct of indirect te identificeren natuurlijke persoon.
  Voorbeeld: naam, geboortedatum, BSN, gevolgde opleiding, type huis waarin iemand woont, gezondheidsgegevens, strafrechtelijke gegevens, gegevens over etnische afkomst;
- Verwerken van persoonsgegevens: iedere handeling met een persoonsgegeven.
  Voorbeeld: ontvangen, lezen, veranderen, doorsturen, opslaan, vernietigen;
- Verwerkingsverantwoordelijke: het college van burgemeester en wethouders is veruit de grootste gemeentelijke verwerkingsverantwoordelijke voor persoonsgegevens.
  Ook de gemeenteraad, de burgemeester, de heffingsambtenaren, de ambtenaren van de burgerlijke stand, de leerplichtambtenaren en de toezichthouders Wmo zijn echter verwerkingsverantwoordelijken; ieder voor zover het de verwerking van persoonsgegevens betreft die plaatsvindt ter uitvoering van één van zijn/hun taken;
- Verwerker: iemand die/een bedrijf dat als dienst persoonsgegevens voor één van de gemeentelijke verwerkingsverantwoordelijken verwerkt.
  Voorbeeld: een salarisadministratiebedrijf, een cloud-provider;
  Voorbeeld uitzondering: een accountant, een zorgaanbieder. Beiden zijn zelfstandig verwerkingsverantwoordelijken;
- Betrokkene: iemand wiens persoonsgegevens binnen de gemeentelijke organisatie worden verwerkt.
  Dit kan een burger, maar ook een medewerker van de gemeente Purmerend zijn;
- Datalek: het verloren gaan of in (intern) onbevoegde handen komen van persoonsgegevens;
- Toestemming: een vrije, specifieke, geïnformeerde en ondubbelzinnige – aantoonbare - verklaring of actie van een betrokkene waaruit blijkt dat hij akkoord gaat met een verwerking van zijn persoonsgegevens;

- Sociaal domein: Dit omvat (diegenen die betrokken zijn bij) de uitvoering van de volgende wetten: Jeugdwet, Wmo 2015, Participatiewet, Wet gemeentelijke schuldhulpverlening en Wet passend onderwijs.

BELANG PRIVACYBELEID

1. Privacybeleid als onderdeel van de privacy governance
Aangegeven wordt hoe dit privacybeleid zich verhoudt tot andere maatregelen die genomen worden om de bescherming van persoonsgegevens een integraal onderdeel van ieders dagelijkse werkzaamheden te maken.

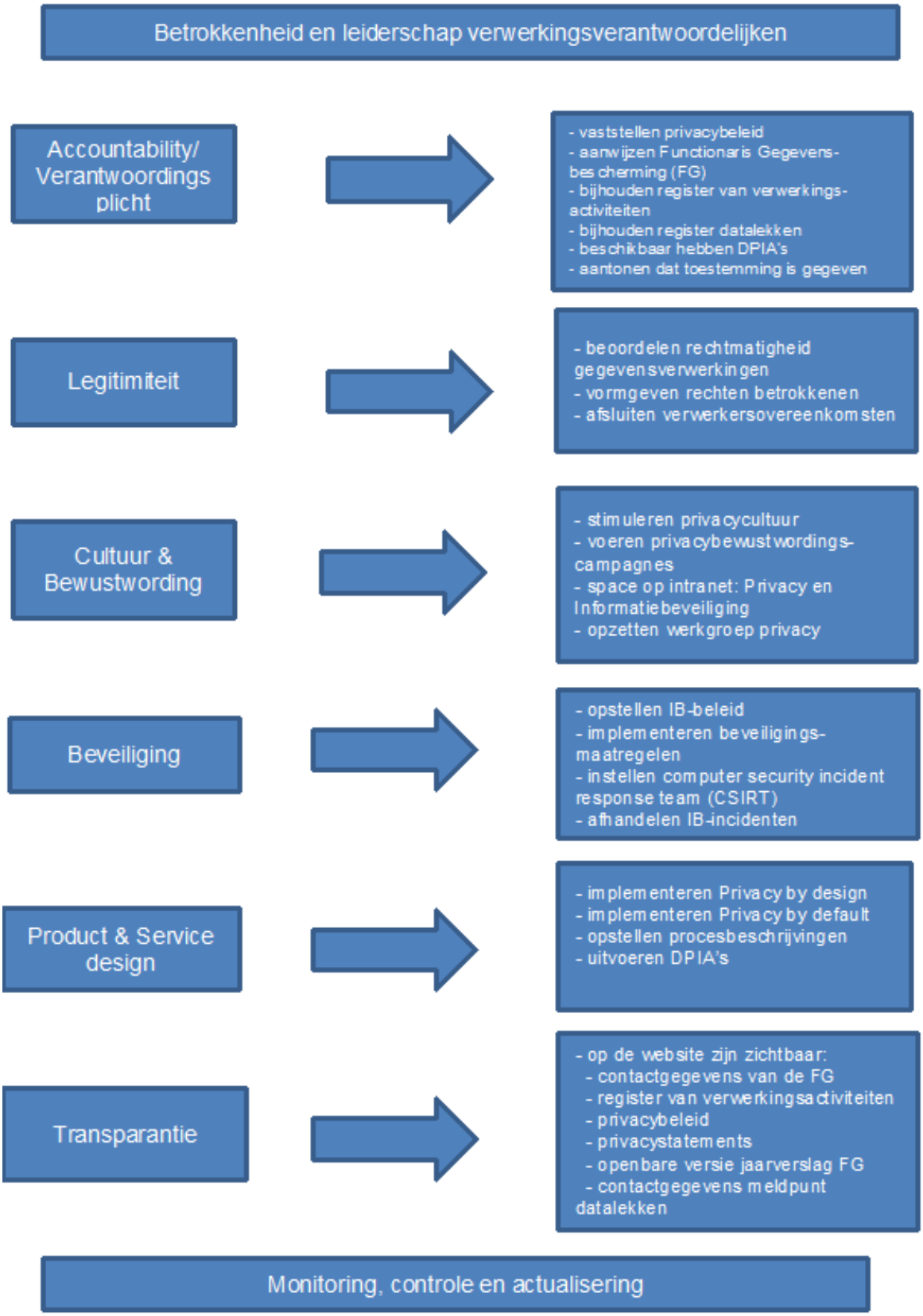
2. Formulering compliance structuur
Aangegeven wordt welke personen, welke rol spelen in bij gemeentelijke privacy gerelateerde onderwerpen.

3. Formulering privacy uitgangspunten
In dit privacybeleid worden door de medewerkers, maar óók door bestuurders en verwerkingsverantwoordelijken zelf, na te leven uitgangspunten geformuleerd.
Deze uitgangspunten moeten er aan bijdragen dat:
- burgers en medewerkers er (meer) vertrouwen in hebben dat hun persoonsgegevens zorgvuldig worden verwerkt;
- de kans op fouten in de omgang met persoonsgegevens vermindert; (daardoor)
- de kans op boetes, aansprakelijkstellingen en corrigerende maatregelen daalt.

Hierbij wordt meteen opgemerkt dat de kans op fouten c.q. op datalekken nooit 0 wordt.
In iedere organisatie worden – onopzettelijk - fouten gemaakt, dus óók in de verwerking van persoonsgegevens. Daarnaast is het onmogelijk altijd alle bedreigingen van buitenaf te weren. Tenslotte kunnen er andere belangen spelen die tot gevolg hebben dat de bescherming van persoonsgegevens hieraan – deels! – ondergeschikt gemaakt wordt.
Voorbeeld: crisissituaties waarbij direct gehandeld moet worden.

PRIVACY GOVERNANCE

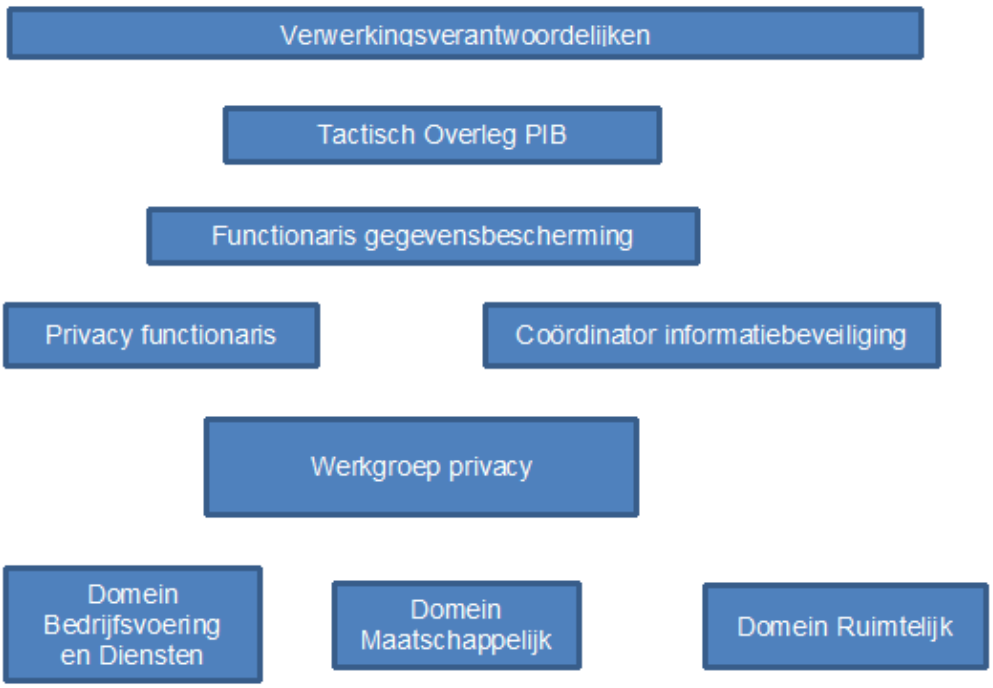
Het privacybeleid staat niet op zichzelf. Het maakt onderdeel uit van een reeks aan maatregelen en documenten om de bescherming van persoonsgegevens binnen de gemeentelijke organisatie te optimaliseren. Deze maatregelen en documenten kunnen gegroepeerd worden rondom 8 elementen c.q. kernbegrippen.
Hierboven werd al gewezen op het IB-beleid. Hiérin zijn de technische en organisatorische beveiligingsmaatregelen opgenomen die ook de te verwerken persoonsgegevens beschermen. Dit IB-beleid wordt geschaard onder het element: Beveiliging.
Er is echter meer. Onderstaand schema maakt dit duidelijk:



Volledig voldoen aan de eisen die de privacywetten aan de gemeentelijke organisatie stellen, betekent voldoen aan c.q. in het bezit zijn van alle in bovengenoemde elementen opgenomen punten/stukken + het actueel houden hiervan via een plan-do-check-act cyclus. Cruciaal hiervoor is een positieve en actieve betrokkenheid van de verwerkings-verantwoordelijken en de directie.

COMPLIANCE STRUCTUUR

De bescherming van persoonsgegevens binnen de gemeentelijke organisatie is geen “speeltje” van een enkeling. Het is een inherent onderdeel van ieders functie/van ieders dagelijks handelen. Tegelijkertijd is de bescherming van persoonsgegevens niet de core business van de meeste medewerkers. Er zijn daarom medewerkers/gremia die advies geven over en toezicht houden op de bescherming van persoonsgegevens binnen de Purmerendse organisatie.
De verhouding tussen de verschillende actoren ziet er als volgt uit:



Tactisch Overleg Privacy&InformatieBeveiliging
Het Tactisch Overleg wordt gevormd door de concerncontrollers van Purmerend en Beemster, de directeur Bedrijfsvoering en Diensten, de managers ICT en Beleid en Projecten, de coördinator informatiebeveiliging, de FG of privacy functionaris en een manager uit elk van de andere domeinen. Het Tactisch Overleg bespreekt team- respectievelijk domeinoverstijgende onderwerpen op de gebieden informatiebeveiliging en privacy. Het Tactisch Overleg kan – al dan niet via de directie – over de besproken onderwerpen adviseren aan de verwerkingsverantwoordelijken.

Functionaris gegevensbescherming
Spil bij privacycompliance in de gemeentelijke organisatie is de FG.
Het hebben van een FG is voor gemeenten vanaf 25 mei 2018 verplicht.
Zijn taken zijn grotendeels vastgelegd in de AVG:

- informeren en adviseren van verwerkingsverantwoordelijken en medewerkers over hun wettelijke verplichtingen in het kader van de bescherming van persoonsgegevens. NB advisering neemt niet de vorm van ondersteuning bij de uitvoering aan;
- toezicht houden op de interne naleving van privacywetgeving en (gemeentelijk) privacybeleid;
- adviseren over en toezien op de uitvoering van gegevensbeschermingseffect-beoordeling (DPIA’s);
- samenwerken met en optreden als contactpunt van de AP;
- aanspreekpunt voor betrokkenen over alle zaken die verband houden met de verwerking van hun gegevens en met de uitoefening van hun rechten o.g.v. de AVG.

Naast deze wettelijke taken:

- is de FG voorzitter van de werkgroep privacy;
- houdt hij samen met de privacy functionaris het register van verwerkingsactiviteiten bij;

- vormt hij samen met de privacy functionaris en de coördinator informatiebeveiliging het Purmerendse meldpunt datalekken;
- is hij sparringpartner van de coördinator informatiebeveiliging voor zover het de beveiliging van persoonsgegevens betreft.

Om de onafhankelijkheid van de FG te benadrukken, wordt hij gepositioneerd bij de Concernstaf en niet bij één van de domeinen.

Privacy functionaris
- Voor medewerkers én voor bestuurders is de privacy functionaris het dagelijkse aanspreekpunt bij vragen over de bescherming van persoonsgegevens voor zover deze niet binnen het domein van de coördinator informatiebeveiliging vallen.
- Ook ondersteunt de privacy functionaris teams bij het opstellen van verwerkersovereenkomsten, het waar nodig mede-implementeren van adviezen van de FG of de privacy functionaris, het opstellen van modellen, zoals een model-toestemmingsbrief.
- Hij is gepositioneerd bij het team Juridische en Veiligheidszaken (JVZ).
- De privacy functionaris is lid van de werkgroep privacy.
- Hij houdt samen met de FG het register van verwerkingsactiviteiten bij.
- De privacy functionaris vormt samen met de FG en de coördinator informatiebeveiliging het Purmerendse meldpunt datalekken.
- De privacy functionaris vervangt de FG bij afwezigheid.

Zoals aangegeven, heeft de FG adviserende én toezichthoudende taken. Het gelijktijdig uitoefenen van beide taken kan spanningen geven. Wanneer dergelijke spanningen voorzienbaar én onwenselijk zijn, kan de privacy functionaris de beantwoording van een concrete adviesvraag van de FG overnemen.

Coördinator informatiebeveiliging (CISO)
- De coördinator informatiebeveiliging stelt het informatiebeveiligingsbeleid en de informatiebeveiligingsplanning op.
- Hij initieert/voert risicoanalyses uit en onderzoekt kwetsbaarheden of laat dit doen.
- Hij handelt informatiebeveiligingsincidenten af en coördineert bij grote beveiligingsincidenten.
- Hij stimuleert de bewustwording binnen en het bewustzijn van de organisatie over informatieveiligheid en risico's.
- Hij vormt samen met de FG en de privacy functionaris het Purmerendse meldpunt datalekken.
- De coördinator informatiebeveiliging adviseert gevraagd en ongevraagd het college, de directie en het lijnmanagement over risico's en te nemen maatregelen.

Werkgroep privacy
Eerder werd gesteld dat de bescherming van persoonsgegevens niet de core business van een medewerker is. Tóch wordt hij geacht zijn taken uit te voeren in overeenstemming met de privacywetten en dit privacybeleid. Het is dus zaak dat een medewerker weet wat er op dit vlak van hem verlangd wordt, dat hij weet waar hij met vragen hierover terecht kan én dat dit laagdrempelig georganiseerd wordt. Verschillende instrumenten kunnen worden ingezet om dit doel te bereiken:
- Hij kan rechtstreeks een beroep doen op de FG of de privacy functionaris, afhankelijk van de vraag die hij heeft;
- Hij kan gebruik maken van de middelen die hem in het kader van cultuur en bewustwording worden aangereikt (zie pag. 4);
- Hij kan zijn vraag via de privacy-ambassadeur binnen zijn team voorleggen aan de werkgroep privacy.

Samenstelling werkgroep
De werkgroep privacy bestaat uit:
- de FG, die voorzitter is;
- de privacy functionaris;
- de coördinator informatiebeveiliging;
- privacy-ambassadeurs, zijnde een medewerker uit elk domein, aangevuld met medewerkers uit de teams die veel persoonsgegevens verwerken, aangewezen door de manager vanwege hun affiniteit met het onderwerp en/of hun werkzaamheden.

Werkwijze werkgroep
- De werkgroep komt eenmaal per 6 weken bij elkaar (of in een andere door de werkgroep wenselijk geachte frequentie).

- Binnen de werkgroep wordt informatie uitgewisseld over alles wat gerelateerd is aan de bescherming van persoonsgegevens binnen de Purmerendse organisatie; dus inclusief informatiebeveiliging van persoonsgegevens.
  Dit kan in de vorm van:
  - bespreking van een vraag van een lid of van een collega uit zijn domein/team;
  - bespreking van knelpunten op een onderdeel van de privacy governance of op een ander privacy gerelateerd onderwerp;
  - bespreking van nieuwe ontwikkelingen op landelijk of gemeentelijk niveau. Denk aan nieuwe richtlijnen van de AP of uit Brussel en de betekenis daarvan voor de dagelijkse Purmerendse praktijk. Denk ook aan nieuwe jurisprudentie met een effect op de gemeentelijke organisatie;
  - presentaties door een externe over privacy-gerelateerde onderwerpen die de werkgroep op dat moment van belang vindt;
  - deelname aan de IBD crisisgame of een ander evenement rondom de bescherming van persoonsgegevens.

- De leden van de werkgroep koppelen de voor hun domein/team relevante informatie uit de werkgroep terug naar hun directe collega's.

PRIVACY UITGANGSPUNTEN

De *AVG* somt in de artikelen 5 en 6 de volgende *beginselen* inzake de verwerking van persoonsgegevens op:
1. Rechtmatigheid, behoorlijkheid, transparantie;
2. Grondslag en doelbinding;
3. Minimale gegevensverwerking;
4. Juistheid;
5. Opslagbeperking;
6. Integriteit en vertrouwelijkheid.

Daar bovenop worden de volgende *gemeentelijke uitgangspunten* geformuleerd:
a. Waar verplicht, worden verwerkersovereenkomsten afgesloten met verwerkers; waar mogelijk, worden privacyconvenanten afgesloten met verwerkingsverantwoordelijken met wie wordt samengewerkt. Aan aanstaande verwerkers wordt de gemeentelijke model-verwerkersovereenkomst aangeboden als uitgangspunt van de onderhandelingen. Dit model is te vinden op de intranet space: Privacy en Informatiebeveiliging.
b. Toestemming wordt alleen als grondslag voor de verwerking van persoonsgegevens gebruikt als er geen andere grondslag aanwezig is. In het sociaal domein wordt van toestemming alleen bij uitzondering gebruik gemaakt.
c. Datalekken worden direct na constatering gemeld aan het Meldpunt datalekken. Bij twijfel omtrent de vraag of sprake is van een datalek, wordt ook met het Meldpunt datalekken contact opgenomen.
d. Vóórdat een nieuwe gegevensverwerking start c.q. bij een ingrijpende wijziging in een bestaande gegevensverwerking, wordt:
   - nagegaan of een DPIA moet worden uitgevoerd;
   - nagegaan of privacy by design dan wel by default mogelijk resp. nodig is;
   - de FG of de privacy functionaris gevraagd het register van verwerkingsactiviteiten bij te werken;
   - gekeken of een aparte privacy statement gemaakt moet worden;
   - gekeken of aparte toestemmingsformulieren opgemaakt moeten worden;
   - nagegaan of een verwerkersovereenkomst afgesloten dan wel gewijzigd moet worden.

e. Betrokkenen worden in staat gesteld hun rechten uit te oefenen.

De verwerkingsverantwoordelijken zijn verantwoordelijk voor de naleving van de AVG beginselen en de gemeentelijke uitgangspunten. Zij moeten kunnen aantonen dat naleving plaatsvindt (de eerder genoemde "accountability"). Zij stellen de FG, de privacy functionaris en de coördinator informatiebeveiliging in staat de medewerkers (en waar nodig de bestuurders en directieleden) bij te staan bij het uitvoeren respectievelijk waarmaken van deze beginselen en uitgangspunten.

VERTALING BEGINSELEN EN UITGANGSPUNTEN IN RICHTLIJNEN VOOR BESTUURDERS EN MEDEWERKERS

Ad 1. Gegevensverwerkingen zijn rechtmatig, behoorlijk, transparant;

- Op het moment dat persoonsgegevens verwerkt worden, is bekend ter uitvoering van welke taak c.q. op basis van welke wet dat gebeurt en welke specifieke eisen deze taak c.q. wet aan de gegevensverwerking stelt.
- Hoe gevoeliger de persoonsgegevens zijn die verwerkt worden, des te zwaarder zijn de technische én organisatorische maatregelen ter bescherming daarvan. Een DPIA (zie onder ad d.) helpt bij de concretisering van de risico's die aan de verwerking verbonden zijn en de maatregelen die ter compensatie of opheffing hiervan genomen moeten worden.
- De betrokkene wordt op het moment van dan wel zo spoedig mogelijk na een eerste verwerking hiervan op de hoogte gesteld, tenzij een wettelijke uitzonderingsgrond deze verplichting (tijdelijk) buiten werking stelt. Waar nodig stelt een team ten behoeve hiervan een specifiek privacy statement op. In ieder geval is ieder domein in het bezit van een generiek privacy statement. Dit privacy statement wordt opgesteld in voor betrokkenen begrijpelijke taal, bevat informatie over de verwerking en wijst betrokkene op zijn rechten. Het privacy statement wordt waar mogelijk gekoppeld aan c.q. (als bijlage) opgenomen in een bestaand (aanvraag)formulier.

Ad 2/b. Grondslag en doelbinding

- Persoonsgegevens worden alleen verwerkt als er voor deze verwerking een doel en een grondslag aanwezig is.
  - Het verwerkingsdoel wordt in een team bepaald.
    Voorbeeld: verwerking t.b.v. de verstrekking van een Wmo voorziening, van een subsidie of van een kapvergunning. Of: verwerking t.b.v. de behandeling van een bezwaarschrift of het afsluiten van een overeenkomst.
  - De grondslagen van een verwerking van persoonsgegevens staan limitatief opgesomd in artikel 6 AVG:
    - Noodzakelijk ter uitvoering van een overeenkomst waarbij de betrokkene partij is;
    - Noodzakelijk om als verwerkingsverantwoordelijke te voldoen aan een wettelijke verplichting.
      Voorbeeld: de verstrekking genoemd in artikel 5.2.2 Wmo 2015 of in artikel 8 Wet gemeentelijke schuldhulpverlening;
    - Noodzakelijk om de vitale belangen van een persoon te beschermen;
    - Noodzakelijk voor de vervulling van een taak van algemeen belang of een taak in het kader van de uitoefening van het openbaar gezag.
      Voorbeeld: jeugdhulp, openbare orde handhaving, afvalinzameling.
    - Toestemming van betrokkene.

- - Toestemming:
    - wordt alleen als grondslag gebruikt als er geen andere grondslag aanwezig is.
    - moet door een betrokkene vrij, specifiek, geïnformeerd en ondubbelzinnig gegeven worden. Informatie aan betrokkene ten behoeve van het geven van toestemming wordt niet alleen verstrekt over de verwerking waarvoor de toestemming gevraagd wordt, maar ook over de dan reeds voorzienbare verdere verwerkingen.
    - mag mondeling gegeven worden, maar het bestaan ervan moet achteraf aantoonbaar zijn. Voorbeeld: door betrokkene ondertekend gespreksverslag. Waar mogelijk wordt gebruik gemaakt van standaard toestemmingsformulieren. Deze (zullen te) vinden zijn op de intranet space: Privacy en Informatiebeveiliging.

  - In het sociaal domein vindt de verwerking van persoonsgegevens in eerste instantie plaats om te voldoen aan een wettelijke verplichting of ter vervulling van een taak van algemeen belang. Bij verwerking van persoonsgegevens bínnen één domein (Jeugdwet, Wmo, Participatiewet), zullen deze twee grondslagen vaak voldoende zijn. Domeinoverstijgende gegevensverwerking (tijdens en n.a.v. keukentafelgesprekken) of verwerking van persoonsgegevens in het kader van vroegsignalering is vrijwel[1] niet geregeld in de domeinwetten. Gegevensverwerking is in die gevallen dan alleen mogelijk als kan worden aangetoond dat een vrije toestemming hiervoor gegeven is; dus een toestemming die niet geregeerd wordt door de afhankelijkheidsrelatie waarin de betrokkene zich t.o.v. de gemeente bevindt. Dit zal niet

1) Uitzondering: artikel 5.2.1 Wmo 2015

snel het geval zijn. Om dit punt concreter te maken, komt op de intranet space: Privacy en Informatiebeveiliging een overzicht van de grondslagen op basis waarvan in het sociaal domein persoonsgegevens verwerkt mogen worden.

Ad 3/5 Minimale gegevensverwerking en opslagbeperking

- Teams verwerken niet meer, maar ook niet minder persoonsgegevens dan noodzakelijk zijn in het kader van het doel waarvoor ze verwerkt worden.
- Wanneer de persoonsgegevens niet langer nodig zijn voor het doel waarvoor ze verwerkt werden, worden ze vernietigd, geanonimiseerd, gepseudonimiseerd of gearchiveerd bij DIV, afhankelijk van de vraag:
  - of ze helemaal niet meer nodig zijn;
  - alleen nog in niet (direct) tot de persoon te herleiden gegevens nodig zijn;
  - de Archiefwet op deze gegevens van toepassing is.

Ad 4. Juistheid

(Persoons)gegevens die worden gebruikt ter uitvoering van een overheidstaak zijn juist en actueel. Dit vereist een actieve houding van het team dat de gegevens verwerkt. Bij twijfel over de juistheid of actualiteit van (persoons)gegevens wordt navraag gedaan bij de betrokkene, een ketenpartner of wordt een basisregistratie geraadpleegd.

Ad 6. Integriteit en vertrouwelijkheid

Maatregelen moeten genomen worden om ervoor te zorgen dat verwerkte persoonsgegevens betrouwbaar zijn en goed beveiligd.
De technische beveiliging van persoonsgegevens in geautomatiseerde systemen wordt geregeld door de teams ICT en Beleid en Projecten.
De organisatorische beveiliging van persoonsgegevens is een taak van de teams zelf.
Voorbeeld: het vergrendelen van een device op het moment dat het achtergelaten wordt; het na werktijd opbergen van papier in een (afgesloten) kast of locker; het verzenden van mails met persoonsgegevens via een beveiligde verbinding.
Het vigerende IB-beleid werkt dit onderwerp verder uit.

Ad a. Verwerkersovereenkomsten en privacyconvenanten

- Artikel 28 AVG verplicht verwerkingsverantwoordelijken:
  - Alleen verwerkers in te schakelen die "afdoende garanties m.b.t. het toepassen van passende technische en organisatorische maatregelen bieden".
    Verwerkers worden in ieder geval geacht deze garanties te bieden als zij op het moment van afsluiten van de overeenkomst gecertificeerd zijn, bijvoorbeeld ISO 27001 en een actuele Verklaring van Toepasselijkheid kunnen overleggen.
  - Met een verwerker die bovenbedoelde garanties biedt, een verwerkersovereenkomst af te sluiten vóórdat de verwerker met zijn werk begint.
    Soms worden verwerkersovereenkomsten voor meerdere verwerkingen afgesloten. Teams die ten behoeve van een nieuwe verwerking een (voor hun nieuwe) verwerker inschakelen, informeren daarom bij de FG of de privacy functionaris of dit het geval is. Er hoeft voor deze nieuwe verwerking dan geen aparte verwerkersovereenkomst afgesloten te worden.

- Met ketenpartners worden veelvuldig persoonsgegevens uitgewisseld. Afspraken omtrent deze uitwisseling kunnen worden vormgegeven in een privacyconvenant. In ieder geval bij de uitwisseling van gevoelige persoonsgegevens wordt met de ketenpartners overlegd of zij bereid zijn afspraken hierover te maken en deze vast te leggen in een privacyconvenant.
  Privacyconvenanten mogen ook worden aangegaan als de samenwerking al enige tijd loopt.
  Voorbeelden van privacyconvenanten worden geplaatst op de intranet space: Privacy en Informatiebeveiliging.
- Periodiek moet worden gecontroleerd of de in een verwerkersovereenkomst of privacyconvenant gemaakte afspraken nog worden nageleefd. In verwerkersovereenkomsten krijgt deze periodieke controle vaak gestalte door de eis dat de verwerker jaarlijks door een onafhankelijke externe deskundige een zgn TPM (Third Party Memorandum) laat afgeven.

Ad c. Datalekken
Het in 2016 ingestelde Meldpunt datalekken ondergaat qua werkwijze geen veranderingen door de (inwerkingtreding van de) AVG. De procesbeschrijving Melden datalekken is als bijlage bij dit beleid gevoegd.
De beantwoording van de vraag of betrokkenen in kennis gesteld worden van een datalek wordt belegd bij de teams, met inachtneming van de door de directie gegeven aanwijzingen, voor zover het een datalek betreft waarvoor het college of de burgemeester de verwerkingsverantwoordelijke is. Het Meldpunt datalekken verzorgt in overleg met de andere verwerkingsverantwoordelijken een eventuele kennisgeving aan betrokkenen.
Wanneer bijzondere persoonsgegevens gelekt zijn, ligt een dergelijke kennisgeving voor de hand. Bij een datalek met andere persoonsgegevens wordt per geval bekeken of een kennisgeving nodig respectievelijk wenselijk is.
Betrokkenen moet in de kennisgeving duidelijk worden gemaakt welke stappen zij kunnen ondernemen om de gevolgen van het datalek voor hén zo klein mogelijk te maken.
Een model van een kennisgevingsbrief wordt geplaatst op de intranet space: Privacy en Informatiebeveiliging.

Ad d. Acties bij nieuwe gegevensverwerking of ingrijpende wijzigingen in bestaande gegevensverwerkingen
Nieuwe (wettelijke) taken brengen vaak nieuwe verwerkingen van persoonsgegevens of wijzigingen in een bestaande verwerking met zich mee. Het is belangrijk in een zo vroeg mogelijk stadium oog te hebben voor en actie te ondernemen op de volgende vraagpunten/onderwerpen:
- houdt de verwerking – waarschijnlijk – een hoog risico in voor de privacy van burgers en/of komt de verwerking voor op de positieve lijst van de AP respectievelijk komt hij niet voor op de negatieve lijst van de AP?
  Voer dan een DPIA uit om te bepalen welke maatregelen genomen moeten worden om die risico's te beperken of weg te nemen en voer die maatregelen – bijvoorbeeld privacy by design - ook uit. Een link naar de DPIA van de IBD wordt op de intranet space: Privacy en Informatiebeveiliging geplaatst. De FG kan hier verder over adviseren.
  Voorbeeld van verwerkingen waarvoor een DPIA moet worden uitgevoerd: verwerkingen in het sociaal domein en verwerkingen bij Team Integrale Veiligheid.
- pas privacy by design/default toe; niet alleen in het ontwerp van een nieuw geautomatiseerd systeem, maar ook in processen.
  Denk hierbij o.a. aan de volgende elementen:
  - regel wie toegang heeft tot de persoonsgegevens onder uitsluiting van anderen. Voorbeeld: via password-beleid en uitgifte van fysieke sleutels tot kasten.
  - pseudonimiseer of zelfs: anonimiseer als de verwerking van de persoonsgegevens zelf niet noodzakelijk is voor de uitvoering van een taak.
  - gebuik de opt-in in plaats van opt-out mogelijkheid.
    Voorbeeld: een burger beslist actief of hij de gemeentelijke nieuwsbrief wil ontvangen. Deze mogelijkheid is niet reeds voor-ingevuld met de mogelijkheid een vinkje uit te zetten.
  - regel een systeem zó in dat het een signaal afgeeft op het moment dat de bewaartermijn bijna is verstreken.

- alleen als de wijziging in een bestaande verwerking gevolgen heeft voor de reeds opgenomen informatie in het register van verwerkingsactiviteiten moet deze geactualiseerd worden.
- maak voor een nieuwe verwerking alleen een specifiek privacy statement of een nieuw toestemmingsformulier als het generieke privacy statement c.q. toestemmingsformulier niet volstaat. De privacy functionaris/FG ondersteunt bij het opstellen hiervan.

Ad e. Rechten van betrokkenen
Betrokkenen hebben op grond van de AVG de volgende rechten:
I. informatie over de verzameling van hun persoonsgegevens;
II. inzage in eigen persoonsgegevens;
III rectificatie van deze gegevens;
IV recht op gegevenswissing/vergetelheid;
V beperking van verwerking van eigen gegevens;
VI dataportabiliteit;
VII recht van bezwaar;
VIII geen onderwerping aan geautomatiseerde besluitvorming.

- Het recht op vergetelheid en op dataportabiliteit zijn nieuw; de overige rechten bestonden al onder de Wbp. De aandacht voor de AVG kan echter tot gevolg hebben dat betrokkenen ook op de al langer bestaande rechten vaker een beroep gaan doen.
- De beslissingen op verzoeken in het kader van deze rechten zijn o.g.v. de Uitvoeringswet besluiten in de zin van de Awb. Een modelbesluit wordt op de intranet space: Privacy en Informatiebeveiliging geplaatst. Tegen dit besluit staat bezwaar en beroep open. Betrokkene kan er voor kiezen tussen de bezwaar- en de beroepsfase de bemiddeling van de AP te vragen.
- Om betrokkenen te wijzen op hun rechten:
- worden op de gemeentelijke website:
    - bovenstaande rechten benoemd met een korte toelichting hierop;
    - modelbrieven geplaatst met behulp waarvan de rechten ingeroepen kunnen worden;
    - - informatie gegeven over de procedure en de beslistermijnen;

- wordt in persoonlijke contacten met betrokkenen waar nodig/desgevraagd:
    - gewezen op deze rechten;
    - verwezen naar de betreffende pagina op de website;
    - aanvullende schriftelijke en/of mondelinge informatie verstrekt.

- Zeker waar rechten dicht bij elkaar liggen (bijvoorbeeld het recht op gegevenswissing en het recht op bezwaar) en/of waar vragen zijn over het te nemen besluit n.a.v. een verzoek van een betrokkene, wordt advies gevraagd aan de privacy functionaris of in algemene zin aan de FG.

Ad I Recht op informatie over verzameling persoonsgegevens
Betrokkenen hebben het recht te weten dat er over hen binnen de gemeente Purmerend persoonsgegevens verwerkt worden.
Betrokkenen van iedere nieuwe verwerking persoonlijk in kennis stellen, vergt een onevenredige inspanning van de medewerkers en maakt het er voor betrokkenen ook niet duidelijker op. Daarom wordt het register van verwerkingsactiviteiten op de gemeentelijke website geplaatst en komen per domein/team privacystatements beschikbaar voor betrokkenen. In deze statements staat specifieke c.q. aanvullende informatie over gegevensverwerkingen, die niet in het register is opgenomen.

Ad II Recht op inzage in eigen persoonsgegevens
Een betrokkene heeft recht op inzage in zijn eigen gegevens.
Een verzoek om inzage in gegevens die bij een specifiek team aanwezig zijn, wordt door dat team afgehandeld.
Een algemeen inzageverzoek in de trant van: “ik wil inzage in alle gegevens die door de gemeente Purmerend over mij verzameld zijn”, wordt gecoördineerd door de privacy functionaris.

Ad III Recht op rectificatie van persoonsgegevens
Een verzoek om rectificatie is meestal een gevolg van het besluit tot inzage in eigen persoonsgegevens. Indien de gegevens ook daadwerkelijk onjuist zijn, worden ze binnen twee weken gerectificeerd door het team dat de persoonsgegevens verwerkt. Zo spoedig mogelijk daarna worden alle ontvangers van de – voorheen onjuiste – persoonsgegevens op de hoogte gesteld van de rectificatie. Hiervan kan slechts worden afgezien als dit écht niet mogelijk is.

Ad IV Recht op gegevenswissing/vergetelheid
Verwerkingsverantwoordelijken hebben de plicht persoonsgegevens te vernietigen, niet langer tot de persoon herleidbaar te maken of te archiveren als ze niet langer het doel dienen waarvoor ze werden verwerkt.
Het verzoek om persoonsgegevens te wissen is het spiegelbeeld van deze plicht.
Op het recht wordt naar verwachting vooral een beroep gedaan als verwerking van de gegevens plaatsvond met toestemming van betrokkene en betrokkene deze toestemming intrekt.
Net als van een rectificatie, worden eerdere ontvangers van een gegevenswissing – zo mogelijk - op de hoogte gesteld.

Ad V Recht op beperking van verwerking van eigen persoonsgegevens
Tijdens de behandeling van een verzoek om rectificatie of bezwaar, kan een betrokkene vragen zijn persoonsgegevens tijdelijk niet te verwerken. Aan dit verzoek wordt gehoor gegeven, bijvoorbeeld door

de persoonsgegevens van betrokkene tijdelijk in een afgezonderd deel van het systeem/het bestand te zetten. In het systeem/bestand wordt vervolgens aangetekend dat de gegevens van betrokkene beperkt verwerkt mogen worden. De beperking wordt opgeheven zodra de reden voor het opleggen daarvan vervalt; bijvoorbeeld omdat een besluit op het verzoek om rectificatie is genomen.

Ad VI Recht op dataportabiliteit

De persoonsgegevens die een betrokkene aan een verwerkingsverantwoordelijke heeft verstrekt én die geautomatiseerd worden verwerkt op grond van toestemming van betrokkene of ter uitvoering van een overeenkomst, moeten op zijn verzoek geautomatiseerd aan hem of – als dit technisch mogelijk is - een andere verwerkingsverantwoordelijke worden verstrekt. Het recht op dataportabiliteit geldt niet voor persoonsgegevens die op basis van andere grondslagen worden verwerkt.
Omdat veel verwerkingen binnen de gemeente Purmerend op basis van een wettelijke verplichting of taak van algemeen belang plaatsvinden, heeft dit recht voor gemeentelijke verwerkingen maar een beperkte betekenis. In het register van verwerkingsactiviteiten kan worden nagegaan op basis van welke grondslagen een verwerking plaatsvindt en of een betrokkene dit recht toekomt.

Ad VII Recht van bezwaar

Een betrokkene kan bezwaar maken tegen het feit dat zijn persoonsgegevens worden verwerkt ter vervulling van een taak van algemeen belang of in het kader van de uitoefening van het openbaar gezag. Hij moet hierbij specifieke omstandigheden aanvoeren, die door de verwerkingsverantwoordelijke moeten worden afgewogen tegen de gerechtvaardigde belangen op voortzetting van de verwerking van de persoonsgegevens van betrokkene.

Ad VIII Recht om niet onderworpen te worden aan geautomatiseerde besluitvorming

De verwerking van persoonsgegevens is mensenwerk. Tenzij een betrokkene hiervoor uitdrukkelijk toestemming geeft of de AVG het expliciet toestaat, mogen persoonsgegevens in het kader van het nemen van een besluit daarom niet door een computer worden verwerkt zonder menselijke tussenkomst. Voorbeeld: een elektronisch ingediende sollicitatiebrief mag niet enkel door een algoritme terzijde worden geschoven; deze brief moet ook door een mens gezien en beoordeeld worden.

NALEVING, MONITORING EN EVALUATIE

Van de verwerkingsverantwoordelijken en hun medewerkers wordt verwacht dat zij de privacywetten en dit beleid naleven (onder de op pag. 2 gemaakte kanttekening). Dit is in het belang van de gemeentelijke organisatie zelf én van degenen wiens gegevens verwerkt worden. Gebeurt dat toch 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 verwerkings-verantwoordelijke corrigerende maatregelen 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 voor een verwerkingsverantwoordelijke c.q. de gemeente Purmerend wanneer bekend wordt dat in strijd met de privacywetgeving is gehandeld.

Dit beleid zal worden geconcretiseerd aan de hand van een nog nader vast te stellen actieprogramma. In dit periodiek/jaarlijks vast te stellen programma zal worden aangegeven welke onderwerpen die periode extra aandacht krijgen.
Voorbeeld van onderwerpen:

- verwerkersovereenkomsten actualiseren/AVG-proof maken;
- bewaar- c.q. vernietigingstermijnen. Vaststelling en naleving daarvan;
- inzagerecht betrokkene. Procesbeschrijving maken en bekendheid aan geven, binnen én buiten de gemeentelijke organisatie.

Voorbeeld extra aandacht:

- thema bijeenkomst in de werkgroep privacy;
- presentatie in teamoverleggen;
- e-learning;
- achtergrondinformatie op intranet;

- artikel in Purmerend Totaal en op gemeentelijke website.

Denkbaar is dat deze extra aandacht ook resulteert in aanpassing van dit beleid.

Ook na 25 mei zullen zich datalekken voordoen en worden er fouten in de verwerking van persoonsgegevens gemaakt.
Door de – op basis van dit beleid gegenereerde – extra aandacht voor dit onderwerp, wordt echter de kans op het maken van fouten verkleind. In zijn jaarlijkse rapportage zal de FG de verwerkingsverantwoordelijken op de hoogte stellen van zijn bevindingen op dit vlak.

Op dit moment worden in de ENSIA al vragen gesteld over privacycompliance. Naar verwachting nemen het aantal vragen over dit onderwerp de komende jaren toe.
De bevindingen uit het ENSIA-traject worden meegedeeld aan de gemeenteraad, aan diverse ministeries en wellicht in de toekomst ook aan de AP. Iedere ontvangende partij kan uit die bevindingen zijn conclusies trekken en de gewenste/noodzakelijke maatregelen treffen. Voor zover het de AP betreft, staan de maatregelen hierboven genoemd. Voor zover het de gemeenteraad betreft, kunnen die gewenste/noodzakelijke maatregelen vertaald worden in een actieprogramma en uiteindelijk in dit beleid.

Purmerend, 1 mei 2018
Burgemeester en wethouders van Purmerend,
de secretaris,
G. Blom
de burgemeester,
D. Bijl
Purmerend, 1 mei 2018
De burgemeester van Purmerend,
D. Bijl