Privacy beleid

Algemeen privacy beleid geldend voor alle organisatieonderdelen van de gemeente Boekel.

Datum: 6 juni 2017

Artikel 1 Definitie en begripsbepalingen

1. Dit beleid strekt tot nadere uitwerking van de Wet bescherming persoonsgegevens (hierna: de Wet). De in de Wet opgenomen definities en overige normen zijn onverkort van toepassing.

2. Dit beleid verstaat onder:
   a. Anonimiseren: persoonsgegevens die voor een taakuitvoering niet meer noodzakelijk zijn, worden verwijderd uit een dataset. De dataset bevat dan enkel geanonimiseerde gegevens, die wel worden bewaard voor bijvoorbeeld onderzoeksdoeleinden of om te gebruiken als open data.
   b. AP: de Autoriteit Persoonsgegevens, op grond van de Wet bescherming persoonsgegevens (WBP) bevoegd om toe te zien op de verwerking van persoonsgegevens overeenkomstig het bij en krachtens de Wet bepaalde.
   c. CIO: Chief Information Officer, zijnde de senior medewerker I&A.
   d. CISO: Chief Information Security Officer, zijnde het hoofd informatiebeveiliging, aangewezen door het college van burgemeester en wethouders.
   e. Dataminimalisatie: alleen de informatie die noodzakelijk is voor de uitvoering van wettelijke taken wordt opgeslagen.
   f. Het DT: directeurenteam, verantwoordelijk voor de verschillende organisatieonderdelen van de gemeente Boekel.
   g. Privacy impact assessment (PIA): een analyse van de gevolgen voor privacy als een project, beleid, dienst, product of ander initiatief wordt gestart of ingevoerd en het nemen van eventueel noodzakelijke mitigerende acties om een negatieve impact te voorkomen dan wel te verkleinen.
   h. Pseudonimiseren: een procedure waarmee identificerende gegevens met behulp van een bepaald algoritme in een dataset worden vervangen door versleutelde gegevens (het pseudoniem).
   i. Tracking: het volgen van mobiele datadragers zoals telefoons, bijvoorbeeld door Wifi- of bluetooth apparatuur waarbij (persoons)gegevens worden verzameld uit die datadragers.

Artikel 2 Uitgangspunten

Het privacy beleid is gebaseerd op de volgende uitgangspunten.

1. Rechtmatigheid

Gegevens van burgers verwerken we binnen de kaders van de geldende wet- en regelgeving en vindt uitsluitend plaats voor zo ver dit nodig is voor een goede gemeentelijke taakuitoefening.

2. Subsidiariteit

Voor het bereiken van het doel waarvoor de persoonsgegevens worden verwerkt, wordt de inbreuk op de persoonlijke levenssfeer zo veel mogelijk beperkt. Als met een ander middel hetzelfde resultaat wordt bereikt, maar minder inbreuk gemaakt wordt op de privacy, dan kiezen we voor dit middel.

3. Proportionaliteit

De inbreuk op de belangen van de betrokkene mag niet onevenredig zijn in verhouding tot het met de verwerking te dienen doel.

4. Werkbaar en zorgvuldig

Het waarborgen van de persoonlijke levenssfeer en de daaruit voortvloeiende wet- en regelgeving, moet tegelijkertijd niet in de weg staan aan een goede en tijdige uitvoering van de gemeentelijke taken, bijvoorbeeld bij zorgverlening of in het kader van de openbare orde en veiligheid. Het beleid voor de verwerking van persoonsgegevens moet met andere woorden niet dusdanig ingewikkeld of rigide zijn, dat het in de weg staat aan de zorg- en dienstverlening.

5. Doelbinding
Gegevens worden gebruikt voor duidelijk omschreven doelen en kunnen alleen worden gebruikt voor andere doelen of worden gedeeld voor zo ver de wet dat toestaat.

6. Transparantie
Er wordt op een transparante wijze gecommuniceerd hoe de gemeente denkt over privacy en hoe de gemeente privacy borgt. De burger wordt in algemene zin proactief geïnformeerd met betrekking tot het privacy beleid.

7. Actualiteit
Gegevens zijn steeds voldoende actueel en zijn een nauwkeurige weergave van de feitelijke situatie. Om dit te borgen worden werkwijzen vastgelegd en op professionele wijze uitgevoerd conform functionele en praktische protocollen en procesbeschrijvingen.

8. Klachten
Klachtenafhandeling vindt plaats via onze reguliere klachtenprocedure.

9. Samenwerking
In geval van samenwerking met externe partners waarbij sprake is van verwerking van persoonsgegevens, worden via een bewerkersovereenkomst afspraken gemaakt over de (beveiligings-)eisen waar gegevensuitwisseling aan moet voldoen, de verplichtingen die de bewerker heeft en met name de verplichting tot het melden van een inbreuk op de beveiliging die leidt tot (een aanzienlijke kans op) ernstige nadelige gevolgen voor de bescherming van persoonsgegevens. Voor bij het werk belangrijke, veel voorkomende processen, worden specifieke procedures beschreven. Daarin wordt voor dat proces aangegeven hoe wordt omgegaan met (privacygevoelige) informatie.

10. Verantwoordelijkheid
De gemeente is altijd (eind)verantwoordelijk voor de gegevensverwerking en de privacy daarvan. Dit geldt ook als gegevens ter beschikking worden gesteld aan derden of worden gedeeld in samenwerkingsverbanden.

Artikel 3 Verantwoordelijkheden

1. Privacybescherming is de verantwoordelijkheid van alle medewerkers en bestuurders van de gemeente Boekel. Er wordt van iedereen verwacht dat ze zich integer gedragen en als de zaak er om vraagt de privacy van betrokkenen te waarborgen.

2. Het College van B&W is eindverantwoordelijke van het privacy beleid en stelt het privacy beleid vast. Privacy en informatieveiligheid vormen een apart item in de paragraaf bedrijfsvoering van de begroting en jaarrekening conform de PDCA-cyclus. Het college legt hiermee verantwoording af aan de raad waar het gaat over de risico’s en beheersmaatregelen met betrekking tot het privacy- en informatiebeveiligingsbeleid.

Artikel 4 Functionaris voor de gegevensbescherming (FG)

1. Het College van B&W benoemt een FG, zoals bedoeld in de Wet, die belast is met toezicht op het privacy- en beveiligingsbeleid van de gemeente.

2. De FG jaagt de implementatie en toepassing van het privacy beleid aan en is verantwoordelijk voor de organisatie brede implementatie van het privacy beleid. Per organisatieonderdeel zijn de interne proceseigenaren hier zelf verantwoordelijk voor.

3. De FG vervult een adviserende rol in specifieke kwesties of bij de totstandkoming van nieuw beleid of de implementatie van wet- en regelgeving. Ook bij calamiteiten of geconstateerde gebreken ligt het op de weg van de FG om de benodigde maatregelen te treffen. De FG rapporteert zo nodig rechtstreeks aan het college van B&W.

4. De FG houdt een register bij van de verschillende melding plichtige gegevensverwerkingen en de door de gemeente gesloten bewerkersovereenkomsten, convenanten en privacy protocollen.

Artikel 5 Privacy binnen interne processen

1. Interne proceseigenaren zoals van de BRP, WMO, Sociale Zaken, Jeugd, openbare veiligheid en P&O zijn verantwoordelijk voor het ontwikkelen, uitvoeren en uitdragen van het privacy beleid binnen hun eigen processen.

2. Onder ontwikkeling, uitvoering en uitdragen van themagericht privacy beleid wordt minimaal verstaan:
   a. Aantoonbare concretisering (documenteren) van beleid in praktische waarborgen, zodat ook op operationeel niveau structureel sprake is van behoorlijke en zorgvuldige verwerking van persoonsgegevens in overeenstemming met de wet.
   b. Het beoordelen van nieuwe of aangepaste verwerkingen in het licht van de meldplicht aan de FG, het uitvoeren van een Privacy impact assessment hiervoor (zie artikel 6) en andere verplichtingen.
   c. De informatiebeveiliging van het organisatieonderdeel. Hieronder vallen in ieder geval:
      - Informatiebeveiligingsbeleid van Boekel opnemen en doorvoeren in contracten met bewerkers en leveranciers;
      - Alle handelingen aangaande de meldplicht datalekken die het organisatieonderdeel aangaan.
   d. De bewustwording binnen het organisatieonderdeel. Proceseigenaren zijn er in praktische zin verantwoordelijk voor dat onder hun proces andere collega's zich bewust zijn en zich gedragen conform de privacywetgeving en dat privacy en informatiebeveiliging besproken wordt in bestaande werkoverleggen. Hierbij wordt bij voorkeur gebruik gemaakt van bestaande oplossingen en structuren, voor zo ver deze inpasbaar zijn.

Artikel 6 Privacy impact assessment (PIA)

1. Voordat een beslissing wordt genomen over nieuwe of wijzigingen van bestaande bewerkingen, wordt door middel van een PIA aangetoond dat de privacy voldoende is gewaarborgd en worden de al dan niet te nemen maatregelen gemotiveerd. De proceseigenaar is verantwoordelijk voor het vooraf uitvoeren van een PIA.

2. De functionaris voor de gegevensbescherming geeft over de PIA een bindend advies.

3. De PIA wordt door de beleidsmedewerker openbaar toegankelijk gemaakt nadat de beslissing als bedoeld onder lid 2 is genomen.

Artikel 7 Open data

1. Hergebruik van gegevens zoals bedoeld in de Wet hergebruik van overheidsgegevens via het aanbieden van open data gebeurt met inachtneming van de Wetgeving en onderliggend beleid.

2. Een openbare dataset bevat geen gegevens die herleidbaar zijn naar een persoon.

3. Van open datasets wordt de status van de dataset voor de afnemer weergegeven op de site waarop de open datasets zijn te verkrijgen.

Artikel 8 Big data en tracking

1. Gegevens in big data en tracking mogen alleen worden verzameld, opgeslagen en gedeeld, als ze niet herleidbaar zijn tot een persoon en worden alleen verzameld voor onderzoek dat door of namens de gemeente wordt uitgevoerd.

2. Voor big data en tracking wordt uitsluitend gebruik gemaakt van brongegevens die door daartoe geautoriseerde personen zijn verzameld.

3. Brongegevens die gebruikt worden voor big data toepassingen worden omgezet tot een dataset die geen persoonsgegevens bevat en dus geanonimiseerd is.

4. Indien het noodzakelijk is om van lid 3 af te wijken wordt vooraf toestemming aangevraagd bij de FG die de aanvraag beoordeeld in het kader van de wet en doelmatigheid. Alleen bij een goedgekeurde aanvraag mogen de gegevens gepseudonimiseerd in plaats van geanonimiseerd worden.

5. Onderzoek aan de hand van de dataset als bedoeld in lid 3, mag alleen door andere dan de in lid 2 bedoelde geautoriseerde personen worden uitgevoerd.

Artikel 9 Cameratoezicht, camerabewaking en overige inzet van camera's

1. Cameratoezicht in de openbare ruimte of waarbij de openbare ruimte geheel of gedeeltelijk in beeld wordt gebracht ten behoeve van de openbare orde of veiligheid vindt alleen door of namens de gemeente plaats, na een daartoe strekkend besluit van de burgemeester.

2. Camerabewaking kan tevens door particuliere bedrijven worden uitgeoefend onder voorwaarde dat indien er camera's in de openbare ruimte worden geplaatst dan wel delen van de openbare ruimte in beeld worden gebracht, er een daartoe strekkend besluit door of namens het college van burgemeester en wethouders is genomen en er een convenant met de verantwoordelijke is gesloten voorafgaande aan de verwerking.

3. Het convenant zoals bedoeld in het tweede lid gaat in ieder geval in op:
   - de grondslag voor de verwerking van persoonsgegevens;
   - het verzamel- en verwerkingsdoel;
   - de organisatorische en technische maatregelen die worden getroffen tegen verlies of onrechtmatige verwerking;
   - de bewaartermijn;
   - de wijze waarop voldaan wordt aan de meldplicht datalekken.

4. Bij inzet van camera's voor andere gemeentelijke doeleinden dient voorafgaand aan deze inzet advies te worden gevraagd aan de FG.

Artikel 10 Datalek

1. Geconstateerde datalekken worden meteen gemeld bij de CISO / FG en de leidinggevende.

2. De verantwoordelijke directeur is verantwoordelijk voor het dichten van het datalek in samenwerking met de CISO / FG.

3. De CISO / FG beoordeelt in samenspraak met de verantwoordelijke directeur of het datalek meldingswaardig is, als bedoeld in de Wet.

4. De CISO / FG meldt een meldingswaardig datalek direct (binnen 72 uur) aan de Autoriteit Persoonsgegevens.

5. De verantwoordelijke directeur is verantwoordelijk voor de onverwijlde melding naar betrokkene(n) wiens persoonsgegevens zijn gelekt.

6. De CISO / FG ziet er met de CIO op toe dat het datalek op adequate wijze wordt gedicht.

Artikel 11 Toezicht

1. Voor de uitoefening van zijn toezichthoudende functie beschikt de FG over alle bevoegdheden die daarvoor redelijkerwijs noodzakelijk zijn. Ingeval van twijfel of verschil van mening daaromtrent beslist de FG, de CIO gehoord hebbende.

2. De verantwoordelijke en de personen die bij een verwerking van persoonsgegevens zijn betrokken verstrekken desgevraagd de FG alle inlichtingen en verlenen alle overige medewerking die hij voor de uitoefening van zijn taak behoeft.

3. De FG heeft toegang tot alle ruimten, waar een verwerking van persoonsgegevens plaatsvind. De FG is bevoegd apparatuur, programmatuur, gegevensbestanden, boeken en bescheiden te onderzoeken en zich de werking van apparatuur en programmatuur te doen tonen.

4. De FG rapporteert over zijn bevindingen aan het college van burgemeester en wethouders. Hij geeft aanbevelingen over te nemen maatregelen, die een goede werking van de verwerking van persoonsgegevens moeten helpen waarborgen.

Artikel 12 Onderzoek

1. De FG kan een onderzoek instellen naar de wijze waarop in verband met de verwerking van persoonsgegevens, in een bepaald geval dan wel in het algemeen belang, de persoonlijke levenssfeer wordt beschermd.

2. De FG kan voor zijn onderzoek gebruik maken van de diensten van derden.

3. De FG deelt zijn bevindingen aan de Verantwoordelijke mede en geeft zo nodig aanbevelingen.

Artikel 13 Register verwerkingen

1. De FG registreert de verwerkingen van persoonsgegevens waarvoor meld- of registratieplicht geldt bij in het daartoe bestemde register.

Artikel 14 Logboek datalekken / beveiligingsincidenten

1. De CISO / FG houdt namens de verantwoordelijke een logboek bij waarin datalekken zijn opgenomen.

2. In het logboek worden in ieder geval de volgende gegevens vermeld:
   a. Het onderwerp van het datalek;
   b. De datum van het datalek;
   c. De duur van het datalek;
   d. De aard van de inbreuk;
   e. De instanties waar meer informatie over de inbreuk kan worden verkregen;
   f. De aanbevolen maatregelen om de negatieve gevolgen van de inbreuk te beperken;
   g. Een beschrijving van de gevolgen voor de verwerkte persoonsgegevens;
   h. De maatregelen die de gemeente heeft getroffen of voorstelt te treffen om deze gevolgen te verhelpen;
   i. De kennisgeving aan betrokkenen.

Artikel 15 Rechten betrokkene

1. De taken zoals omschreven in artikel 35 van de WBP en volgende worden centraal uitgevoerd onder verantwoordelijkheid van de CIO.

2. Bij uitoefening van de taken wordt de FG betrokken.

3. Een betrokkene kan een verzoek zoals beschreven in artikel 35 eerste lid van de Wet ook via andere gangbare publieksdienstverleningskanalen van de gemeente Boekel doen. Dit verzoek is geldig ongeacht het middel waarmee het verzoek wordt gedaan.

Artikel 16 Inwerkingtreding

1. Dit beleid treedt in werking met ingang van de dag na vaststelling.

Bijlage 1. Toelichting

Artikel 1 Definitie en begripsbepalingen
Pseudonimiseren is noodzakelijk indien datasets vergeleken moeten worden. Dit wordt bijvoorbeeld gedaan binnen het sociaal domein. De gemeente wil de zorg die wordt geboden door de instellingen controleren door gericht onderzoek waarbij vaak meerdere datasets worden gebruikt.

Artikel 2 Uitgangspunten
De uitgangspunten als genoemd in dit beleid zijn van toepassing op alle taken en processen waar de gemeente voor verantwoordelijk is.

Artikel 3 Verantwoordelijke
Het college van burgemeester en wethouders dan wel de burgemeester zijn, iedere vanuit hun eigen bevoegdheid, is te allen tijde verantwoordelijke voor de verwerkingen en bewerkingen die door of namens de gemeente worden uitgevoerd.

Artikel 4 Functionaris voor de gegevensbescherming
De gemeente heeft een functionaris voor de gegevensbescherming (FG) benoemd die verantwoordelijk is voor het toezicht op privacy en de borging er van. Hij kan het college van burgemeester en wethouders, de burgemeester en de gemeenteraad gevraagd en ongevraagd advies geven over privacy-aangelegenheden. De FG heeft verregaande bevoegdheden op grond van de Wbp. Binnen de gemeente Boekel vervult de FG tevens de rol als CISO.

In artikel 63 lid 2 wordt zijn onafhankelijke rol benadrukt:
De FG kan wat betreft de uitoefening van zijn functie geen aanwijzingen ontvangen van de verantwoordelijke of van de organisatie die hem heeft benoemd. Hij ondervindt geen nadeel van de uitoefening van zijn taak. De verantwoordelijke stelt de FG in de gelegenheid zijn taak naar behoren te vervullen. De FG kan de kantonrechter verzoeken te bepalen dat de verantwoordelijke gevolg dient te geven aan hetgeen in de tweede volzin is bepaald. Hoewel de FG een eigen rol kent, treedt hij altijd in overleg met de CIO over geconstateerde gebreken of onjuistheden in het systeem van verwerkingen.

Tot de taken van de FG behoren in ieder geval:
a. Toezicht op de verwerking van persoonsgegevens door de gemeente Boekel.
b. Gevraagd en ongevraagd signaleren, adviseren en informeren over zaken aangaande de Wet, het privacy beleid en overige onderwerpen die de privacy betreffen.
c. Toezicht houden op het gemeentelijk privacy- en beveiligingsbeleid door middel van advisering en controles.
d. Inventarisatie van de verwerkingsprocessen en beheren van meldingen van verwerkingen in het register van de Autoriteit Persoonsgegevens.
e. Verantwoordelijke voor de coördinatie van de werkprocessen in geval van datalekken en het beheren van het logboek inzake datalekken.
f. Aanspreekpunt en contactpersoon aangaande privacy, zowel intern als extern.

Artikel 5 Privacy binnen interne processen
De proceseigenaar is verantwoordelijk voor de uitvoering van diverse processen binnen een specifiek organisatieonderdeel. Hij of zij is verantwoordelijk voor borging van de privacy en informatiebeveiliging bij het betreffende organisatieonderdeel. De contactpersonen hebben regelmatig overleg met de FG / CISO en zorgen voor eenduidige uitvoering van het privacy- en informatiebeveiligingsbeleid door het organisatieonderdeel.

Artikel 6 Privacy Impact Assessment (PIA)
Voordat wordt besloten om een verwerking van persoonsgegevens te starten of te wijzigen, wordt door de proceseigenaar van het organisatieonderdeel een privacy impact assessment (PIA) uitgevoerd. Uitgangspunt bij een PIA is dat afhankelijk van de verwerking passende waarborgen worden ingebouwd (Privacy by Design). Bij iedere verwerking van persoonsgegevens wordt dataminimalisatie toegepast. Daarnaast worden binnen die minimale dataset - waar mogelijk - de persoonsgegevens eerst geanonimiseerd en de overige persoonsgegevens worden gepseudonimiseerd. Deze keuzes worden onderbouwd voorgelegd aan de FG, die mede beslist over de inhoud van de PIA.

De PIA legt in de eerste plaats de risico's bloot van projecten waarbinnen wordt gewerkt met persoonsgegevens, en het draagt bij aan het vermijden of verminderen van deze privacy risico's. Op basis van de antwoorden die worden gegeven in de PIA wordt op systematische wijze inzichtelijk gemaakt of er een kans is dat de privacy van de betrokkene wordt geschaad, hoe groot deze kans is en op welke gebieden dit speelt.

De PIA doet dit op een gestructureerde wijze:
- De mogelijk (negatieve) gevolgen van het gebruik van persoonsgegevens voor de betrokken personen en organisaties in kaart te brengen.
- De risico's voor de betrokken personen en organisaties zoveel mogelijk te lokaliseren.

Op basis van de uitkomsten van de PIA kan de gemeente gericht acties ondernemen om deze risico's te verminderen. Door het gebruik van de PIA kan bescherming van persoonsgegevens op een gestructureerde manier onderdeel uitmaken van de belangenafweging en besluitvorming over een project.

De PIA is openbaar met inachtneming van de Wet openbaarheid van bestuur. In ieder geval worden de volgende gegevens van verwerkingen bij navraag bekend gemaakt:
a. De reden om de persoonsgegevens te bewaren;
b. Bewaartermijnen en een motivering waarom voor die bewaartermijn gekozen is met zo mogelijk een verwijzing naar het wettelijk kader;
c. Mogelijke uitzonderingen op de gekozen bewaartermijn met uiteenzetting van de voorwaarden waaronder langer bewaard kan worden;
d. Een verwijzing naar de persoon bij wie een betrokkene een verzoek kan indienen als hij inzage wil hebben in verwerkingen die hem aangaan.

Er zal gebruik worden gemaakt van de PIA die door de Informatie Beveiliging Dienst (IBD) wordt aanbevolen. De IBD is onderdeel van het KwaliteitsInstituut Nederlandse Gemeenten (KING).

De FG ziet toe op het proces en geeft een bindend advies over de PIA.

Artikel 7 Open data
Om het begrip Open data te definiëren is aansluiting gezocht bij het Platform Open Data. Zij omschrijft open data als data die vrij gebruikt kunnen worden, hergebruikt kunnen worden en opnieuw verspreid kunnen worden door iedereen - onderworpen enkel, in het uiterste geval, aan de eis tot het toeschrijven en gelijk delen.

Kenmerken van open data:
- Beschikbaarheid en Toegankelijkheid: De data moet in zijn geheel beschikbaar zijn, en voor niet meer dan een redelijke productieprijs, bij voorkeur door middel van downloaden via het internet. De data moet ook beschikbaar zijn in een handige en modificeerbare vorm.
- Hergebruik en herverspreiding: de data moet aangeboden worden onder voorwaarden die hergebruik en herverspreiding toestaan, daarbij ook het samenvoegen met andere datasets inbegrepen.

- Universele deelname: iedereen moet kunnen gebruiken, hergebruiken en herverspreiden. Er moet geen discriminatie bestaan tegen velden van een bepaalde onderneming, of tegen personen of groepen. Bijvoorbeeld, ‘niet-commerciële’ beperkingen die ‘commercieel’ gebruik voorkomen, of beperkingen voor het gebruiken van de data voor bepaalde doeleinden (e.g. alleen in het onderwijs), zijn niet toegestaan.

De gemeente heeft veel data die onder voorwaarden opengesteld kan worden voor een breed publiek. Hier zijn ook verschillende redenen voor aan te wijzen:
- Data waar (overheids-)organisaties over beschikken vertegenwoordigen waarde voor anderen;
- Veel verschillende groepen mensen en organisaties kunnen profiteren van de beschikbaarheid van open data, inclusief de overheid zelf;
- Het is onmogelijk om precies te voorspellen hoe en waar de waarde van deze data zal ontstaan in de toekomst. De aard van innovatie is dat ontwikkelingen vaak uit onverwachte hoek komen.

Economisch gezien is open data ook van groot belang. Verscheidene onderzoeken hebben de economische waarde van open data geschat op miljarden Euro.

De overheid heeft ook een taak als het gaat om hergebruik van overheidsgegevens. In de Wet hergebruik van overheidsgegevens zijn voorwaarden bepaald waaronder hergebruik kan plaatsvinden. Het privacy beleid stelt de eisen voor de gemeente Boekel waaraan het gebruik van open data moet voldoen. Hergebruik is immers niet altijd wenselijk of toelaatbaar. Naast beperkingen door wet- en regelgeving is het ook niet de bedoeling dat gegevens waarin persoonsgegevens zijn verwerkt worden hergebruikt en daarmee beschikbaar gesteld als open data.

Een afnemer moet van de status van de data uit kunnen gaan en dat de data voldoen aan bepaalde kwaliteitseisen. Dit is immers ook van belang voor de toepassing waarvoor hij de open data gebruikt. Er is geen wettelijke verplichting om datasets bij te houden en te actualiseren bij het aanbieden ervan. Daarom is in het Privacy beleid de verplichting opgenomen dat het betreffende organisatieonderdeel aangeeft welke status de dataset heeft.

Artikel 8 Big data en tracking
Dit artikel is bedoeld om de mogelijkheden van tracking en big data in te kaderen voor de gemeente. Big data en tracking kunnen van onschatbare waarde zijn voor de organisatie. Het gebruik ervan mag echter niet leiden tot het herleidbaar zijn van personen. Hierbij geldt de volgende volgordelijkheid: op een dataset vindt eerst dataminimalisatie plaats, vervolgens wordt anonimisering zoveel mogelijk toegepast en alleen als het noodzakelijk is om datasets te vergelijken wordt pseudonimiseren toegepast.

Doel van tracking is om publieksstromen (aantallen) in kaart te brengen en daarop eventuele regulerende maatregelen te kunnen treffen. Voor big data en tracking is het niet nodig dat persoonsgegevens kenbaar zijn. Het is ook nadrukkelijk niet de bedoeling dat de persoonsgegevens voor andere doeleinden dan deze worden gebruikt. Big data en tracking van mobiele gegevensdragers worden uitsluitend toegepast als de privacy van het individu kan worden gewaarborgd. Daar waar gegevens tot personen herleidbare informatie leidt of kan leiden wordt deze informatie onherkenbaar gemaakt op zodanige wijze dat herleiding niet meer mogelijk is.

Gelet op de grootschaligheid van big data biedt dit beleid een extra waarborg voor de veilige verwerking van de persoonsgegevens. Het verzamelen van de (persoons)gegevens voor big data mag niet door dezelfde personen worden uitgevoerd als degenen die het onderzoek met behulp van die (gepseudonimiseerde) gegevens uitvoeren. De verzamelde gegevens worden geanonimiseerd of gepseudonimiseerd door de bronhouder, de geautoriseerde persoon namens gemeente. De versleutelde dataset wordt door de bronhouder aan de onderzoeker toegestuurd. De onderzoeker krijgt zodoende datasets die voor hem niet meer herleidbaar zijn naar persoonsgegevens. Hij krijgt geen beschikking over het (onversleutelde) brondocument.

Het verschil tussen anonimiseren en pseudonimiseren van persoonsgegevens ziet met name op de bruikbaarheid van deze gegevens voor het vergelijken van databestanden. Bij anonimiseren worden alle persoonsgegevens verwijderd uit de dataset. Hierdoor zijn personen, adressen of plaatsen niet meer te herleiden. Wanneer de gemeente uit verschillende datasets een analyse wil (laten) maken van een wijk is dat met een geanonimiseerde dataset niet mogelijk. De relevante gegevens zijn dan immers uit de dataset verdwenen. Dan is pseudonimisering noodzakelijk.

Bij pseudonimisering worden de persoonsgegevens (door toepassing van een algoritme) vervangen door bijvoorbeeld een nummer. Hierdoor zijn de persoonsgegevens niet meer te herleiden. Maar door toepassing van het algoritme kunnen wel meerdere datasets naast elkaar gebruikt worden voor een gerichte analyse van bijvoorbeeld een wijk, zonder dat er persoonsgegevens worden verwerkt. Ook voor meerjarige onderzoeken waarbij datasets over meerdere jaren vergeleken moeten worden biedt pseudonimisering de (enige) mogelijkheid om onderzoek veilig uit te voeren.

De geanonimiseerde en/of gepseudonimiseerde datasets zijn altijd kopieën van de bronbestanden. De gemeente heeft immers een wettelijke taak om bepaalde (persoons)gegevens te bewaren gedurende een langere termijn. Dat een dataset wordt geanonimiseerd en/of gepseudonimiseerd ten behoeve van een onderzoek gedurende die bewaartermijn doet daaraan niet af. Het is daarom niet toegestaan om het bronbestand na anonimisering te vernietigen. Uitsluitend na ommekomst van de bewaartermijn wordt het bronbestand vernietigd.

Artikel 9 Cameratoezicht en camerabewaking

Cameratoezicht
Cameratoezicht vindt plaats op basis van artikel 151 subc van de Gemeentewet. Er kan enkel sprake zijn van cameratoezicht, als er een wettelijke basis is. De inzet van cameratoezicht moet evenredig zijn in relatie tot het doel (proportionaliteit) en mag nooit een doel op zich zijn. Het inzetten van cameratoezicht is één van de zwaarste middelen dat in aanvulling op een pakket aan maatregelen kan worden ingezet. Vast moet staan dat het doel niet op een minder ingrijpende wijze kan worden bereikt (subsidiariteit). Door een analyse te maken van de veiligheidssituatie van een locatie wordt bekeken welke maatregelen een bijdrage kunnen leveren om het probleem aan te pakken. Het inzetten van cameratoezicht is altijd een besluit van de burgemeester, afgestemd met de Driehoek (burgemeester, hoofd van politie, officier van justitie).

Het is een tijdelijke maatregel waarbij periodiek wordt geëvalueerd waar de camera's hangen, met welk doel ze op die locatie geplaatst zijn en of zij nog steeds bijdragen aan dat doel. Die doelen zijn maatwerk en verschillen per gebied. De camerabeelden zijn door fysieke, softwarematige en organisatorische maatregelen beveiligd. Ze mogen alleen onder directe politieaansturing door een kleine groep opgeleide en gescreende functionarissen worden bekeken. De beelden worden maximaal 28 dagen opgeslagen en daarna automatisch gewist. In die 28 dagen kan de politie beelden van strafbare feiten terugzoeken en gebruiken voor opsporing. Met de camera’s kan niet in woningen worden gekeken. Er wordt met software een grijs vlak over de woning gelegd dat meedraait als de camera beweegt (‘blanking’). Opgeslagen beelden vallen onder de Wet Politiegegevens.

Camerabewaking
Naast toezichtcamera’s zijn er ook talloze andere camera’s. Bijvoorbeeld camera’s ter bewaking van eigendommen en verkeerstelcamera’s. Camerabewaking in iemands eigendom is altijd mogelijk: kom je als dief een huis binnen dan moet je niet raar opkijken als je gefilmd wordt. Anders wordt het als de openbare ruimte wordt mee gefilmd en persoonsgegevens op die manier worden verkregen. De openbare ruimte is van iedereen maar het eigendom ligt veelal bij de gemeente.

Omdat bij camerabewaking vaak ook (een deel van) de openbare weg wordt gefilmd is de gemeente partij. Zij moet voor het filmen toestemming verlenen en daarbij komt dat die toestemming niet altijd wettelijk geregeld is (doelbinding). De gemeente moet verzoeken van bedrijvencollectieven, winkels

en gelijke partijen om camerabewaking te installeren afwegen aan de hand van alle belangen en de Wet. Bij bijvoorbeeld bedrijvencollectieven die bedrijventerreinen laten filmen ter voorkoming van vernieling en diefstal speelt het algemeen belang een rol. Hier kan de gemeente worden gevraagd om toestemming voor het filmen van een deel van de openbare ruimte.

Om voor de inwoners duidelijkheid te geven hoe omgegaan wordt met camerabewaking in de openbare ruimte moet een kader worden gesteld. Gekozen is om een convenant verplicht te stellen zodat voor gemeente altijd duidelijk is wat een camera doet in een bepaald gebied. De aanvragers kunnen een cameraplan overleggen met een motivering waarom camerabewaking voor het gevraagde doel past binnen de Wet en het privacy beleid. Omdat het openbare ruimte betreft moeten de aanvragers ook de voorwaarden van de gemeente volgen die op de camerabewaking van toepassing worden. Daarom wordt altijd een convenant gesloten indien er sprake is van camerabewaking door derden waarbij de openbare ruimte wordt gefilmd.

Voorwaarden kunnen bijvoorbeeld zijn: bij het gebruik van camera's in combinatie met opslag van het beeldmateriaal is in veel gevallen sprake van het verwerken van persoonsgegevens. Hierbij wordt de duur van de opslag van de verzamelde beelden in tijd zodanig beperkt dat dit overeenkomt met het doel van de verwerking.

Bij inzet van camera's moet voorafgaand aan de plaatsing worden bepaald voor welk doel de camera wordt ingezet, de duur van de inzet, de bewaartermijn van de beelden alsmede de toegang tot de beelden. Beelden zijn uitsluitend toegankelijk voor hiertoe geautoriseerde personen en worden niet aan derden verstrekt.

Alleen indien beelden dusdanig vaag worden opgeslagen waardoor directe of indirecte herkenning van personen niet meer mogelijk is (ook niet door middel van achteraf uit te voeren beeldverbeteringstechnieken) is geen sprake van verwerken van persoonsgegevens. Ook bij camera inzet voor andere gemeentelijke doeleinden dient voorafgaand aan deze inzet de impact op de privacy duidelijk te zijn. Bijvoorbeeld als bij verkeerskundig onderzoek gebruik wordt gemaakt van camera's.

Artikel 10 Datalek
Op 1 januari 2016 is de Wet bescherming persoonsgegevens gewijzigd als gevolg van de Wet meldplicht datalekken en uitbreiding bestuurlijke boetebevoegdheid van de Autoriteit Persoonsgegevens (hierna te noemen AP). Belangrijk gevolg hiervan is dat organisaties verplicht zijn om een inbreuk op de beveiliging te melden, wanneer het lekken een ernstig nadelig gevolg kan hebben op de bescherming van verwerkte persoonsgegevens. De melding moet aan de AP worden gedaan. In sommige gevallen moeten zelfs de betrokkenen op de hoogte worden gebracht wiens persoonsgegevens zijn gelekt. Bijvoorbeeld als de inbreuk ongunstige gevolgen voor de betrokkenen met zich mee brengt. Indien de regels niet of onvoldoende worden nageleefd kan de AP een forse boete opleggen.

Zowel private als publieke organisaties worden verplicht om inbreuken in de beveiliging die leiden tot verlies, misbruik of diefstal, te melden bij de AP, indien het lekken een ernstig nadelig gevolg kan hebben op de bescherming van verwerkte persoonsgegevens. Melding dient binnen 72 uur plaats te vinden. Melden mag ook later maar dan moet gemotiveerd worden waarom de melding is uitgesteld. Daarnaast moet ook degene wiens persoonsgegevens het betreft een melding krijgen, wanneer er (waarschijnlijk) sprake zal zijn van ongunstige gevolgen voor zijn/haar privacy.

Wat is een datalek?
Er is sprake van een datalek als het gaat om een beveiligingslek waarbij persoonsgegevens in handen vallen van derden die geen toegang tot die persoonsgegevens mogen hebben. Persoonsgegevens zijn alle gegevens die direct of indirect naar personen zijn te herleiden. Een datalek is het gevolg van een beveiligingsprobleem of een gebruikersfout. In de meeste gevallen gaat het om uitgelekte computerbestanden, al kan een gestolen geprinte klantenlijst evengoed een datalek vormen.

Wanneer is er sprake van inbreuk op de beveiliging?
Een inbreuk op de beveiliging hoeft niet te betekenen dat de beveiliging is tekortgeschoten. Denkbaar is dat de beveiliging op zich van voldoende niveau is, maar dat de beveiligingsmaatregelen worden omzeild. In de toelichting bij de wet worden als voorbeeld genoemd: een hack van een ICT-systeem dat persoonsgegevens bevat en de diefstal van een laptop of mobiele telefoon uit een afgesloten kluisje.

Daarnaast kan de inbreuk op de beveiliging het gevolg zijn van een tekortschietende beveiliging. Dat is bijvoorbeeld het geval als bepaalde bestanden niet goed beveiligd zijn geweest of als er menselijke fouten zijn gemaakt. Als voorbeelden kunnen worden genoemd: het slordig omgaan met wachtwoorden, papieren dossiers die als oud papier worden aangeboden, het kwijtraken van apparaten of gegevensdragers met privacygevoelige informatie, een USB-stick, laptop, tablet, telefoon. Ook het onversleuteld elektronisch uitwisselen van privacygevoelige informatie valt hieronder, bijvoorbeeld via e-mail of andere onbeveiligde verbindingen.

Op de hierboven genoemde situaties is de meldplicht van toepassing. Uitsluitend wanneer de getroffen voorzieningen niet specifiek bedoeld zijn voor de beveiliging van persoonsgegevens hoeft geen melding te worden gedaan. In de toelichting bij de wet wordt het voorbeeld genoemd van een gebouw dat afbrandt als gevolg van blikseminslag, waarbij persoonsgegevens verloren zijn gegaan.

De gemeente verwerkt veel persoonsgegevens van inwoners om haar taken uit te kunnen oefenen. Inwoners hebben recht op bescherming van hun persoonsgegevens. Daarom is de gemeente verplicht om persoonsgegevens goed te beveiligen. Met de meldplicht wordt bijgedragen aan het behoud en herstel van vertrouwen in de omgang met persoonsgegevens.

Ook voor partijen die in opdracht van de gemeente persoonsgegevens verwerken (bewerkers) brengt de wet indirect verplichtingen met zich mee. Denk bijvoorbeeld aan leveranciers van ICT-systemen. Hier dienen schriftelijke afspraken over te zijn gemaakt, zodat bij een eventueel datalek de gemeente onmiddellijk wordt ingelicht door de dienstverlener om te bepalen of er daadwerkelijk een datalekmelding moet worden gedaan. De leverancier zal de gemeente dan per ommegaande moeten waarschuwen als zij een inbreuk vaststelt.

De Autoriteit Persoonsgegevens kan bij nalatigheid om aan haar te melden, een boete opleggen als genoemd in artikel 66 van de wet. NB: deze boete staat los van de boete die geldt voor het datalekken zelf. Afhankelijk van de aard en omvang van het datalek kan de AP hiervoor een boete opleggen als genoemd in artikel 66 van de wet.

Wie meldt een datalek?
Iedereen kan aan de gemeente Boekel een datalek melden. Zowel interne medewerkers als externen die een mogelijk datalek constateren moeten bij de gemeente Boekel een melding doen van het datalek aan de FG of leidinggevende.

Meldingsplicht of niet
Niet elk datalek moet bij de AP worden gemeld. Nodeloze meldingen moeten worden voorkomen. Er dient aan bepaalde criteria te worden voldaan. De FG bepaald of een melding aan de AP noodzakelijk is aan de hand van criteria die door de AP zijn vastgesteld. De FG houdt een overzicht bij van de datalekken. Dit overzicht wordt, vanuit archief technisch oogpunt, permanent bewaard.

De meldingsdossiers (meldingsformulier en andere relevante stukken) over datalekken worden gedurende zeven jaar na het vervallen van het belang bewaard.

Artikel 11 Toezicht
De FG is belast met het toezicht op alle privacyaspecten binnen de gemeente Boekel. Hij beoordeelt zelfstandig of de gemeente voldoet aan de Wet en deze verordening. Zijn bevoegdheden zijn verstrekkend. Hij kan in het uiterste geval een beslissing overrulen. Dit zal alleen het geval zijn als duidelijk is dat de Autoriteit Persoonsgegevens ook niet kan instemmen met de betreffende beslissing op privacy gebied.

De FG zal bij een privacy issue altijd eerst via de lijn proberen de situatie op te lossen. Vervolgens zal het DT worden gevraagd de beslissing aan te passen en ten slotte zal interventie plaatsvinden met de gemeentesecretaris. Hoewel de FG een eigen rol kent, treedt hij wel altijd in overleg met de CIO over geconstateerde gebreken of onjuistheden in het systeem van verwerkingen.

Artikel 12 Onderzoek
De FG kan een onderzoek instellen naar (schendingen van) privacyaspecten door de gemeente Boekel. Hij kan hiervoor derden inschakelen die vertrouwelijk met de persoonsgegevenskwestie om kunnen gaan, zoals bijvoorbeeld een accountant die vanuit zijn professie een geheimhoudingsplicht kent. Het onderzoek en mogelijke aanbevelingen worden openbaar gemaakt via de website. Er kunnen dringende redenen zijn om openbaarmaking vooralsnog achterwege te laten, zoals bijvoorbeeld in het geval het college eerst verregaande maatregelen moet treffen om een mogelijke privacy schending te voorkomen.

Artikel 13 Register verwerkingen
De FG registreert alle verwerkingen in een register. Door het aanstellen van een FG is er geen verplichting om de verwerkingen te registreren bij de Autoriteit Persoonsgegevens.

Artikel 14 Logboek datalekken
De FG / CISO houdt een logboek bij van datalekken / beveiligingsincidenten. Het logboek is op te vragen. De FG / CISO houdt bij opname in het register rekening met de belangen die bij openbaarmaking zijn gemoeid. Er kunnen bijvoorbeeld redenen zijn om openbaarmaking aan te houden, zoals bijvoorbeeld bij een ernstig datalek dat eerst moet worden gedicht.

Artikel 15 Rechten betrokkene
Betrokkenen kunnen de gemeente verzoeken om inzage te geven in de verwerkingen van hun persoonsgegevens. Dit kan schriftelijk per post of per email. Hierdoor kunnen meldingen van vermeende datalekken, vragen over PIA’s, klachten, rechten als opvragen, wijzigen, vernietiging van persoonsgegevens ook laagdrempelig worden gedaan.