Gemeente Borger-Odoorn

GEMEENTEBLAD

Officiële uitgave van de gemeente Borger-Odoorn

Nr. 59431

13 maart

2019

Privacy reglement gemeente Borger-Odoorn

Inleiding

In dit reglement laat gemeente Borger-Odoorn zien op welke manier zij dagelijks omgaat met persoonsgegevens en privacy, en wat er wettelijk wel en niet verantwoord is.

In de bijlage zijn de gouden regels van de gemeente Borger-Odoorn te vinden. De gouden regels betreffen de praktische uitvoering van het verwerken van persoonsgegevens.

1. Wetgeving en definities

De Algemene Verordening Gegevensbescherming (AVG) regelt samen met de Uitvoeringswet AVG en de specifieke materiewetten het juridische kader voor de omgang met persoonsgegevens in Nederland.

De volgende begrippen worden in de AVG gebruikt (artikel 4 van de AVG):

Anonimiseren: persoonsgegevens die voor een taakuitvoering niet meer noodzakelijk zijn, worden verwijderd uit een dataset. De dataset bevat enkel geanonimiseerde gegevens.

Autoriteit Persoonsgegevens (AP): de AP is op grond van de AVG bevoegd om toe te zien op de verwerking van persoonsgegevens.

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

Gegevensbeschermingseffectbeoordeling **:** met een gegevensbeschermingseffectbeoordeling worden de effecten en risico's van de nieuwe of bestaande verwerkingen beoordeeld op de bescherming van de privacy. Dit heet ook wel een Data Protection Impact Assessment (DPIA).

Persoonsgegevens: Alle gegevens die gaan over mensen en waaraan je een mens als individu kunt herkennen. Het gaat hierbij niet alleen om vertrouwelijke gegevens, zoals over iemands gezondheid, maar om ieder gegeven dat te herleiden is tot een bepaald persoon (bijvoorbeeld: naam, adres, geboortedatum). Naast gewone persoonsgegevens kent de wet ook bijzondere persoonsgegevens. Dit zijn gegevens die gaan over gevoelige onderwerpen, zoals etnische achtergrond, politieke voorkeuren of het Burgerservicenummer (BSN).

Pseudonimiseren **:** een procedure waarmee identificerende gegevens met behulp van een bepaald algoritme in een dataset worden vervangen door versleutelde gegevens (het pseudoniem).

Verwerker: De persoon of organisatie die de persoonsgegevens verwerkt in opdracht van een andere persoon of organisatie.

Verwerking: Een verwerking is alles wat je met een persoonsgegeven doet, zoals: vastleggen, bewaren, verzamelen, bij elkaar voegen, verstrekken aan een ander of vernietigen.

Verwerkingsverantwoordelijke: Een persoon of instantie die alleen, of samen met een ander, het doel en de middelen voor de verwerking van persoonsgegevens vaststelt.

2. Reikwijdte

Het reglement is van toepassing op alle verwerkingen van persoonsgegevens door alle bestuursorganen van de gemeente. Oftewel: voor alle verwerkingen die binnen de gemeente plaatsvinden. Dit privacy reglement vormt een verdere uitwerking van de wet- en regelgeving en een praktische handleiding voor de organisatie. Het geeft de regels en uitgangspunten voor de eerlijke, zorgvuldige en rechtmatige verwerking van persoonsgegevens. Op die manier kan hiermee een nog betere verwerking van persoonsgegevens plaatsvinden binnen de gemeentelijke organisatie.

3. Verantwoordelijke voor de verwerking

De bestuursorganen van de gemeente zijn allemaal verwerkingsverantwoordelijken voor de verwerkingen die in opdracht van hun worden uitgevoerd. De bestuursorganen van de gemeente zijn de burgemeester, het college van burgemeester en wethouders (college van B&W) en de gemeenteraad.

4. Verwerkingen

De verwerking van persoonsgegevens is elke handeling of elk geheel van handelingen met persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde processen (artikel 4 van de AVG). De gemeente verzamelt en verwerkt persoonsgegevens, omdat de gemeente diensten verleent aan klanten, bedrijven en haar eigen personeel. In de AVG valt onder een verwerking:

- Verzamelen, vastleggen en ordenen;
- Bewaren, bijwerken en wijzigen;
- Opvragen, raadplegen, gebruiken;
- Verstrekken door middel van doorzending;
- Verspreiding of enige andere vorm van ter beschikking stellen;
- Samenbrengen, met elkaar in verband brengen;
- Afschermen, uitwissen of vernietigen van gegevens.

5. Doeleinden

Volgens de wet mogen persoonsgegevens alleen verzameld worden als daarvoor een doel is vastgesteld (artikel 5 van de AVG). Het doel moet uitdrukkelijk omschreven en gerechtvaardigd zijn. Ook moet steeds nagegaan worden of het verwerken van persoonsgegevens noodzakelijk is voor het doel. De gegevens mogen niet voor andere doelen verwerkt worden. Voor de uitvoering van sommige wetten, zoals bijvoorbeeld de Jeugdwet, zijn de doelen voor het verwerken in de wet al vastgelegd, net als de persoonsgegevens die gevraagd en verwerkt mogen worden. Daar waar over verwerking van persoonsgegevens in bijzondere wetgeving niets is geregeld, gelden de regels van de AVG (en de daarmee samenhangende Uitvoeringswet AVG).

6. Rechtmatige grondslag

De wet zegt dat er voor elke verwerking van persoonsgegevens een rechtmatige grondslag uit de wet van toepassing moet zijn (artikel 6 van de AVG). Dat betekent dat de verwerking alleen mag plaatsvinden:

- Om een verplichting na te komen die in de wet staat;
- Voor de uitvoering van een overeenkomst waarbij de betrokkene partij is;
- Om een ernstige bedreiging voor de gezondheid van de betrokkene te bestrijden (vitaal belang);
- Voor de goede vervulling van de gemeentelijke taak;
- Wanneer de betrokkene toestemming heeft gegeven voor de specifieke verwerking.

Voor alle grondslagen zal er altijd een noodzaak moeten zijn om die gegevens te verwerken. Of het verwerken van bepaalde gegevens noodzakelijk is, moet altijd gemotiveerd worden. Van de zes grondslagen zijn voor de gemeente in de praktijk veelal de wettelijke grondslag en de goede vervulling van de gemeentelijke taak leidend. Doordat er tussen de gemeente en de klant een afhankelijkheidsrelatie bestaat, zal de grondslag toestemming zelden kunnen worden gebruikt. Voor veel voorzieningen moet de klant aankloppen bij de gemeente en is de klant afhankelijk van de overheid. Alleen in uitzonderlijke situaties of als de wet dat vereist is toestemming van de klant een grondslag.

7. Wijze van verwerking

De hoofdregel van de verwerking van persoonsgegevens 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. Dit betekent dat verwerking alleen is toegestaan wanneer het doel niet op een andere manier kan worden bereikt.
In de wet wordt ook gesproken over proportionaliteit. Dit betekent dat persoonsgegevens alleen mogen worden verwerkt als dit in verhouding staat tot het doel. Wanneer met geen, of minder (belastende), persoonsgegevens hetzelfde doel bereikt kan worden moet daar altijd voor gekozen worden.

De gemeente zorgt ervoor dat de persoonsgegevens kloppen en volledig zijn voordat ze verwerkt worden. Deze gegevens worden alleen verwerkt door personen met een geheimhoudingsplicht of personen die een integriteitsverklaring hebben ondertekend. Daarnaast beveiligt de gemeente alle persoonsgegevens. Dit moet voorkomen dat de persoonsgegevens kunnen worden ingezien of gewijzigd door iemand die daar geen recht toe heeft. Hoe de gemeente dit doet staat in het informatiebeveiligingsbeleid van de gemeente en in een eventueel aanvullend beveiligingsplan specifiek opgesteld voor een proces of registratie.

8. Doorgifte aan derden

Persoonsgegevens mogen in principe niet worden doorgegeven aan een organisatie in een land buiten de EU (artikel 44 t/m 50 van de AVG). Dit komt omdat binnen de EU een goede bescherming voor de persoonsgegevens is, en daarbuiten niet in alle gevallen. Onder doorgifte wordt o.a. verstaan: het opslaan (bijvoorbeeld in de 'Cloud') of het ter beschikking stellen aan een organisatie buiten de EU. Hieronder valt niet het via internet zichtbaar maken van persoonsgegevens aan personen buiten de EU. De gemeente geeft alleen persoonsgegevens door aan een land buiten de Europese Economische Ruimte (EER) of een internationale organisatie op grond van goedgekeurde afspraken door de Europese Commissie.

9. Transparantie en communicatie

Communicatie, openheid en toetsing zijn belangrijke randvoorwaarden voor het realiseren van een optimale inbedding van het privacy reglement. Richting de klant is communicatie over gegevensbescherming van belang. De klant heeft het recht te weten wat er met zijn of haar gegevens gebeurt (informatieplicht). Het gaat hierbij niet alleen om informatie over de manier waarop de gemeente met persoonsgegevens omgaat maar ook om informatie over de rechten van inwoners, zoals inzage- en correctierecht van gegevens, de mogelijkheid verzet aan te tekenen tegen verwerking en het vernietigingsrecht als wel informatie over de bezwaar- en klachtenprocedure.

9.1 Wet openbaarheid van bestuur (Wob)
Via de Wob kan een ieder een verzoek om informatie indienen bij de gemeente. Bij het verzoek bekijkt de gemeente altijd of het antwoord geen inbreuk maakt op de persoonlijke levenssfeer van betrokkenen. In principe worden geen persoonsgegevens verstrekt. Er wordt altijd een belangenafweging gemaakt of persoonsgegevens wel of niet worden verstrekt.

9.2 Wet hergebruik van overheidsinformatie
De Wet hergebruik van overheidsinformatie regelt het op verzoek verstrekken van overheidsinformatie voor hergebruik. Bij het verzoek bekijkt de gemeente altijd of het antwoord geen inbreuk maakt op de persoonlijke levenssfeer van betrokkenen. In principe worden geen persoonsgegevens verstrekt.

9.3 Informatieplicht (artikel 13, 14 van de AVG)
De gemeente informeert betrokkenen over het verwerken van persoonsgegevens. Wanneer betrokkenen gegevens aan de gemeente geven, worden zij op de hoogte gesteld van de manier waarop de gemeente met persoonsgegevens om zal gaan. Dit kan bijvoorbeeld via een formulier gebeuren. Vaak staat op de aanvraagformulieren vermeld welke gegevens zonder toestemming niet openbaar gemaakt zullen worden. De betrokkene wordt niet nogmaals geïnformeerd als hij/zij al weet dat de gemeente persoonsgegevens van hem/haar verzamelt en verwerkt, en weet waarom en voor welk doel dat gebeurt.

Wanneer de gegevens via een andere weg gekregen worden, dus buiten de betrokkene om, wordt de betrokkene geïnformeerd op het moment dat deze voor de eerste keer worden verwerkt.

9.4 Bewaartermijn
De gemeente bewaart de persoonsgegevens niet langer dan nodig is voor de uitvoering van gemeentelijke taken, of zoals vastgelegd in de Archiefwet. Wanneer er nog persoonsgegevens opgeslagen zijn die niet langer nodig zijn voor het bereiken van het doel worden deze zo snel mogelijk verwijderd. Dit houdt in dat deze gegevens vernietigd worden, of zo worden aangepast dat de informatie niet meer gebruikt kan worden om iemand te identificeren.

9.5 Rechten van betrokkenen (artikel 13 t/m 20 van de AVG)
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:
- Recht op informatie: betrokkenen hebben het recht om aan de gemeente te vragen of zijn/haar persoonsgegevens worden verwerkt.
- Inzagerecht: betrokkenen hebben de mogelijkheid om te controleren of, en op welke manier, zijn/haar gegevens worden verwerkt.
- Correctierecht: als duidelijk wordt dat de gegevens niet kloppen, kan de betrokkene een verzoek indienen bij de gemeente om dit te corrigeren.
- Recht van verzet: betrokkenen hebben het recht aan de gemeente te vragen om hun persoonsgegevens niet meer te gebruiken.
- Recht om vergeten te worden: in gevallen waar de betrokkene toestemming heeft gegeven om gegevens te verwerken, heeft de betrokkene het recht om de persoonsgegevens te laten verwijderen.
- Recht op bezwaar: betrokkenen hebben het recht om bezwaar te maken tegen de verwerking van zijn/haar persoonsgegevens. De gemeente zal hieraan voldoen, tenzij er gerechtvaardigde gronden zijn voor de verwerking.

9.6 Indienen van verzoek
Om gebruik te maken van zijn/haar rechten kan de betrokkene een verzoek indienen. Dit verzoek kan zowel schriftelijke als digitaal ingediend worden. De gemeente heeft één maand de tijd, vanaf de ontvangst van een (compleet) verzoek, om te beoordelen of het verzoek gerechtvaardigd is. Binnen één maand zal de gemeente laten weten wat er met het verzoek gaat gebeuren. Als het verzoek niet wordt opgevolgd is er de mogelijkheid om bezwaar te maken bij de gemeente, of een klacht gerelateerd aan de AVG in te dienen bij de Autoriteit Persoonsgegevens (AP) of de Functionaris Gegevensbescherming.

9.6.1 Identificatie
Alvorens een verzoek in behandeling wordt genomen, dient de betrokkene te worden geïdentificeerd. De gemeente gaat zorgvuldig om met de gegevens van betrokkenen en wil daarom vaststellen dat de gegevens aan de juiste persoon worden overhandigd. Om bijvoorbeeld fraude te voorkomen, is het nodig dat betrokkene langskomt om zich te identificeren met zijn/haar identificatiebewijs. Het opsturen van een kopie van het identiteitsbewijs acht de gemeente onvoldoende om de identiteit vast te stellen. Indien de identiteit van betrokkene niet kan worden vastgesteld, kan de gemeente geen gevolg geven aan het verzoek van betrokkene.

10. Plichten van de gemeente
10.1 Register van verwerkingen (artikel 30 van de AVG)
De gemeente is verantwoordelijk voor het aanleggen van een register van alle verwerkingen waarvan de gemeente de verwerkingsverantwoordelijke is. Elk register bevat een beschrijving van wat er tijdens een verwerking plaatsvindt, en welke gegevens daarvoor worden gebruikt, namelijk:
- De naam en contactgegevens van de verwerkingsverantwoordelijke en, mogelijk, de gezamenlijke verwerkingsverantwoordelijke;
- De doelen van de verwerking;
- Een beschrijving van het soort persoonsgegevens en de daarbij horende betrokkenen;
- Een beschrijving van de ontvangers van de persoonsgegevens;
- Een beschrijving van het delen van persoonsgegevens aan een derde land of internationale organisatie;
- De termijnen waarin de verschillende persoonsgegevens moeten worden gewist;
- Een algemene beschrijving van de beveiligingsmaatregelen.

10.2 Privacy by design en privacy by default (artikel 25 van de AVG)
Bij de aanschaf of ontwikkeling van producten, systemen of processen moet altijd rekening worden gehouden met de bescherming van persoonsgegevens. We noemen dit privacy by design en privacy by default. Voor alle producten, systemen of processen moeten de technische en organisatorische maatregelen ervoor zorgen dat standaard alleen die gegevens worden gebruikt die nodig zijn voor het doel. Bij het ontwerp van een systeem of werkwijze wordt aandacht besteed aan de wijze waarop waarborgen voor de naleving van de AVG kunnen worden ingebouwd, zoals de toegang tot de persoonsgegevens en automatische archivering, verwijdering en vernietiging.

10.3 Gegevensbeschermingseffectbeoordeling (artikel 35 van de AVG)
Met een gegevensbeschermingseffectbeoordeling (DPIA) worden de effecten en risico's van nieuwe of bestaande verwerkingen beoordeeld op de bescherming van de privacy. De gemeente voert deze uit wanneer er een geautomatiseerde verwerking, een grootschalige verwerking, of wanneer er een grootschalige monitoring van openbare ruimten plaatsvindt. Dit geldt in het bijzonder bij verwerkingen waarbij nieuwe technologieën en gevoelige of bijzondere persoonsgegevens worden gebruikt.

10.4 Meldplicht datalekken (artikel 33, 34 van de AVG)
We spreken van een datalek wanneer persoonsgegevens in handen vallen van derden die geen toegang tot die gegevens mogen hebben. Wanneer er een datalek heeft plaatsgevonden meldt de gemeente dit zonder onredelijke vertraging, uiterlijk 72 uur nadat er kennis van de inbreuk is vernomen, aan de AP. Deze melding is niet noodzakelijk als het niet waarschijnlijk is dat de inbreuk in verband met persoonsgegevens een risico inhoudt voor de rechten en vrijheden van natuurlijke personen. Als dit later dan 72 uur is, wordt er een motivering voor de vertraging bij de melding gevoegd. Het kan zijn dat de inbreuk een hoog risico met zich meebrengt voor de rechten en vrijheden van de betrokkenen. In dit geval meldt de gemeente dit aan de betrokkenen in eenvoudige en duidelijke taal. Om toekomstige datalekken te voorkomen worden bestaande datalekken geëvalueerd.

10.5 Functionaris voor de Gegevensbescherming (FG) (Artikel 37 t/m 39 van de AVG)
De gemeente heeft een FG aangesteld. De FG wordt door de gemeente actief betrokken bij alle aangelegenheden die verband houden met de bescherming van persoonsgegevens. De taken van de functionaris zijn informeren, adviseren, toezicht houden, bewustwording creëren, en optreden als contactpersoon van de AP. De functionaris is niet verantwoordelijk voor de uitvoering van de taken op het gebied van bescherming van de privacy. De afdelingen hebben hun eigen verantwoordelijkheid in het goed omgaan met privacygevoelige gegevens. Een verwerking van persoonsgegevens wordt eerst aan de FG gemeld voordat de verwerking begint. De FG is verantwoordelijk voor het toetsen van de implementatie en de uitvoering van de wettelijke eisen en de gemeentelijke richtlijnen op het gebied van privacy door de gemeente.

Voor vragen over privacy of over dit reglement kunt u contact opnemen met de Functionaris voor de Gegevensbescherming van de gemeente Borger-Odoorn via:
E-mailadres: fg@borger-odoorn.nl of gemeente@borger-odoorn.nl t.a.v. de Functionaris voor de gegevensbescherming.
Telefoonnummer: 14 0591
Postadres: Postbus 3, 7875 ZG Exloo

10.6 Contactpersonen privacy per afdeling/cluster
Per afdeling/cluster zullen contactpersonen privacy zijn aangewezen door leidinggevenden. De personen hebben meer uitleg gekregen over de AVG, waardoor zij dienen als eerste vraagbaak op de afdelingen. Indien deze contactpersonen niet kunnen adviseren, kan de jurist privacy of de functionaris gegevensbescherming geraadpleegd worden. Tevens hebben deze contactpersonen een actieve rol bij het up-tot-date houden van het register van verwerkingen.

Bekendmaking en inwerkingtreding

Dit reglement treedt in werking na vaststelling door het college van burgermeester en wethouders. Het reglement wordt geëvalueerd en, indien nodig, herzien. Als er belangrijke wijzigingen zijn, wordt het privacy reglement bijgesteld.

Exloo, 20 februari 2019

Gouden regels voor zorgvuldig en veilig omgaan met (persoons-)gegevens

Om voor iedereen op een duidelijke en begrijpelijke wijze het belang van het zorgvuldig omgaan met persoonsgegevens onder de aandacht te brengen, zijn er 10 regels opgesteld. Deze regels gelden niet alleen binnen de 'muren' van de gemeente Borger-Odoorn, maar uiteraard ook als je thuis of op een andere locatie werkt. Ook gelden deze regels voor de Stichting Sociale Teams Borger-Odoorn.
Deze 10 regels worden gezamenlijk aangeduid als de gouden regels voor zorgvuldig en veilig omgaan met (persoons-)gegevens. Iedereen binnen de gemeente Borger-Odoorn en de Stichting Sociale Teams Borger-Odoorn dient deze gouden regels te kennen, te respecteren en toe te passen in de dagelijkse werkzaamheden.

De 10 gouden regels zijn:

1. **Behandel persoonsgegevens vertrouwelijk en integer;**
   - Iedereen heeft recht op eerbiediging van zijn persoonlijke levenssfeer en een zorgvuldige omgang met zijn persoonsgegevens*;
   - Persoonsgegevens mogen alleen worden verzameld en verwerkt* (zo)als het in ons 'register van verwerkingen' is aangegeven;
   - Gegevens moeten correct en actueel zijn. Zorg ervoor dat gegevens niet (meer) zijn worden gewist of gecorrigeerd;
   - Ben je er van bewust dat toestemming van betrokkenen* voor verwerking van gegevens voor ons geen rechtmatige grondslag is als betrokkenen afhankelijk is van ons besluit (niet in vrijheid gegeven). Dit geldt bijna ook altijd voor het delen van gegevens.

2. **Ga zorgvuldig met (persoons)gegevens om;**
   - Berg na werktijd alle stukken met persoonsgegevens op in afgesloten kasten;
   - Bespreek vertrouwelijke zaken op de juiste plaats en denk na over de informatie die je deelt;
   - Laat geen documenten liggen bij de multifunctionals en neem ook de originelen mee.

3. **Ga (veilig) met (persoons)gegevens om;**
   - Vergrendel je computer als je je plek verlaat, ook als je kort van je plek bent;
   - Laat, als je van je plek gaat, ook geen persoonsgegevens liggen;
   - Persoonsgegevens moeten worden beschermd tegen ongeoorloofde of onrechtmatige verwerking en tegen onopzettelijk verlies, vernietiging, beschadiging of diefstal;
   - Houd wachtwoorden geheim;
   - Gebruik beveiligde papiercontainers als je informatie met persoonsgegevens wilt weggooien. Gooi vertrouwelijke documenten niet thuis bij het oud papier, maar neem ze mee naar kantoor voor vernietiging.

4. **Verwerk niet meer persoonsgegevens dan nodig;**
   - Verwerk alléén gegevens die **noodzakelijk** zijn voor het bereiken van het doel: let daarbij altijd op de proportionaliteit (evenredigheid tot doel) en subsidiariteit (doel op minst ingrijpende manier bereiken).
   - Er zijn veel klanten die ons zonder enige beperking voorzien van álle (bijzondere) persoonsgegevens die ze bezitten. Noteer en rapporteer (ook dan) alleen de gegevens die strikt noodzakelijk zijn voor je taak (b.v. benoem alleen dat er (bepaalde) belemmeringen zijn die in de weg staan bij arbeidsinschakeling en vermeld eventueel dat je bewijs hebt ingezien);
   - Verwerk **geen persoonsgegevens waaruit** iemands ras of etnische afkomst, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen, het lidmaatschap van een vakbond, gegevens over gezondheid, gegevens met betrekking tot iemands seksueel gedrag of seksuele gerichtheid blijken.

5. **Motiveer en leg vast wat je doet;**
   - Deel of ontvang je gegevens? Leg dan ook vast dat, wat en door/aan wie het gedeeld is;
   - Houd altijd rekening met de rechten van betrokkene (o.a. informatie, inzage, rectificatie, verwijdering).

6. **Leg uit waarom we persoonsgegevens verwerken en wees transparant;**
   - Als je vraagt om persoonsgegevens, leg dan aan betrokkene uit waarom en waarvoor de persoonsgegevens worden verwerkt (of waarom juist níet) en wat dit betekent;
   - Wij verzamelen veel gegevens van en over personen. Een persoon waarover wij gegevens verzamelen heeft het recht om te weten wat wij met de gegevens doen en wat wij over de

persoon verwerken. Dit staat ook in ons privacyverklaring (website) en in ons register van verwerkingsactiviteiten.

7. **Weet wanneer je persoonsgegevens mag delen met anderen;**
   - Delen van persoonsgegevens is **verboden**, tenzij dit op grond van een verplichting of bevoegdheid wél mag **en** het delen noodzakelijk is;
   - Verzeker je er (altijd) van of je gegevens mág delen. Ben je bewust van de consequenties als gegevens onterecht worden gedeeld. Binnen de gemeente Borger-Odoorn kan het per rol verschillen wat je mag delen. Twijfel je? Raadpleeg dan altijd het register van verwerkingsactiviteiten op de website.

8. **Ken de risico's van e-mail, internet en sociale media;**
   - Bij het verzenden van een e-mail waarin persoonsgegevens staan, moet je altijd gebruik maken van **'veilig verzenden'**. Dit doe je door de e-mail te verzenden via de knop 'veilig verzenden'. Dit moet zowel intern als extern;
   - Verzend nooit lijsten of persoonsgegevens naar externe personen of bedrijven (zonder toestemming van je coördinator of teamleider);
   - Check altijd of de ontvangers van een e-mail de informatie ook écht moeten hebben;
   - Controleer bij het doorsturen van e-mail of de hele inhoud, dus ook eventuele bijlages, voor de ontvanger(s) bestemd is;
   - Wees zakelijk, vriendelijk en discreet op sociale netwerken zoals LinkedIn, Facebook en Twitter.

9. **Ga verantwoord om met mobiele faciliteiten;**
   - Neem mobiele apparaten waar gegevens opstaan mee of berg ze afgesloten op: zoals smartphones, tablets en USB-sticks;
   - Ga zorgvuldig om met mobiele apparatuur en voorkom verlies of diefstal;
   - Beveilig je mobiele apparatuur met een sterk wachtwoord;
   - Zorg dat waardevolle informatie van je mobiele apparatuur regelmatig wordt opgeslagen op het netwerk van de gemeente;
   - Sla nooit persoonsgegevens op op je eigen laptop/computer of telefoon.

10. **Maak melding van beveiligingsincidenten.**
    - Een inbreuk in verband met persoonsgegevens (een datalek*) kan voor betrokkenen grote gevolgen hebben, waaronder verlies van controle over hun persoonsgegevens, beperking van hun rechten, discriminatie, identiteitsdiefstal of financiële verliezen;
    - Voorbeelden van incidenten: verlies IPhone, verlies documenten, ongeautoriseerd gebruik, verzending (delen) persoonsgegevens naar b.v. een verkeerd (e-mail-) adres en of persoon etc.;
    - Heb je een lek of incident geconstateerd? Neem altijd onverwijld contact op met je coördinator of teamleider en meld dit bij privacy@borger-odoorn.nl
    - Na melding wordt beoordeeld:
      - Wie en hoe het incident/lek aangepakt moet worden;
      - of het incident gemeld moet worden aan de Autoriteit persoonsgegevens.

Jurist privacy: Anne Hulshof
Functionaris gegevensbescherming: Harry de Groot
CISO: Ronald Schotanus
Contactpersoon privacy Sociale Teams: Anne-Marie Keizer

* **begripsbepalingen**:
Betrokkene: degene op wie een Persoonsgegeven betrekking heeft.
Persoonsgegeven: alle gegevens die betrekking hebben op een geïdentificeerde of identificeerbare natuurlijke persoon. Dit betekent dat informatie ofwel direct over iemand gaat, ofwel naar deze persoon te herleiden is.
Het verwerken van Persoonsgegevens: De verwerking van persoonsgegevens is elke handeling of elk geheel van handelingen met persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde processen. In de AVG valt onder een verwerking:
- Verzamelen, vastleggen en ordenen
- Bewaren, bijwerken en wijzigen
- Opvragen, raadplegen, gebruiken
- Verstrekken door middel van doorzending

- Verspreiding of enige andere vorm van ter beschikkingstellen
- Samenbrengen, met elkaar in verband brengen
- Afschermen, uitwissen of vernietigen van gegevens

Datalek : elke inbreuk op de beveiliging van de Persoonsgegevens, die per ongeluk of op onrechtmatige wijze heeft geleid tot de vernietiging, het verlies, de wijziging of de ongeautoriseerde toegang tot, de ongeautoriseerde verstrekking van of het ongeautoriseerde gebruik van doorgezonden, opgeslagen of anderszins verwerkte Persoonsgegevens, inclusief geconstateerde incidenten of kwetsbaarheden waarin dergelijk verlies, toegang, verstrekking, gebruik of verwerking redelijkerwijs niet kan worden uitgesloten. Voorbeelden zijn verlies van een USB-stick of computer, inbraak door een hacker, verzending van email waarin de e-mailadressen van alle geadresseerden zichtbaar zijn voor andere geadresseerden, een malwarebesmetting of een calamiteit, zoals brand in een datacentrum.