gemeente
Montfoort

Privacybeleid gemeente Montfoort 2024

Inleiding
Binnen de gemeente Montfoort wordt veel gewerkt met persoonsgegevens van inwoners, ondernemers, medewerkers (inclusief inhuur/externen) en (keten) partners. Persoonsgegevens zijn alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon. Dit betekent dat informatie ofwel direct over iemand gaat, ofwel naar deze persoon te herleiden is.

Deze persoonsgegevens gebruikt/verzamelt de gemeente voor het goed kunnen uitvoeren van de overheidstaken. Denk hierbij onder andere aan taken in het sociaal domein, openbare orde en veiligheidsdomein of voor burgerzaken. Om deze taken goed te volbrengen is het noodzakelijk dat de gemeente persoonsgegevens verwerkt. Inwoners, ondernemers, medewerkers en (keten)partners moeten erop kunnen vertrouwen dat wij zorgvuldig en veilig met deze persoonsgegevens omgaan.

Nieuwe technologische ontwikkelingen, innovatieve voorzieningen, globalisering en een steeds digitaler wordende overheid maakt het zorgvuldig omgaan met persoonsgegevens steeds complexer.

Doel
Met dit privacybeleid geeft de gemeente een kader voor het verantwoord omgaan met persoonsgegevens en het waarborgen van de persoonlijke levenssfeer van de personen waarvan de gemeente persoonsgegevens verwerkt (of laat verwerken).

De Algemene Verordening Gegevensbescherming (hierna: AVG) en de Wet politie gegevens (hierna: Wpg) zijn daarbij het centrale kader. Daarnaast is het privacy beleid bedoeld om de belangen van betrokkenen – meestal zijn dit de inwoners van de gemeente Montfoort – centraal te stellen. Betrokkenen kunnen met behulp van dit document meer informatie krijgen over de manier waarop wij persoonsgegevens verwerken.

De verdere uitwerking van dit beleid is - waar relevant - vastgelegd in de operationele documenten binnen de gemeente, zoals handreikingen, concrete werkprocedures of werkafspraken voor algemene onderwerpen zoals datalekken, maar ook domeinspecifieke onderwerpen als gegevensdeling voor de uitvoering van de Jeugdwet of de Wet Maatschappelijke Ondersteuning.

Naast dit door het college vastgestelde privacybeleid is een informatiebeveiligingsbeleid vastgesteld. Hierin zijn maatregelen opgenomen om de beschikbaarheid, integriteit en vertrouwelijkheid van (persoons)gegevens te garanderen. Informatiebeveiliging is een randvoorwaarde voor de bescherming van persoonsgegevens. Het gemeentelijke privacybeleid kan daarom niet los worden gezien van het gemeentelijke informatiebeveiligingsbeleid.

Reikwijdte
De gemeente verzamelt en gebruikt persoonsgegevens van inwoners, leveranciers en medewerkers en andere natuurlijke personen (hierna te noemen: betrokkenen).

Dit privacybeleid is van toepassing op alle verwerkingen van persoonsgegevens door of namens de gemeente, waaronder:
1. De verwerking van persoonsgegevens binnen de bedrijfsprocessen van de gemeente;
2. De verwerking van persoonsgegevens die is uitbesteed, of op een andere manier is georganiseerd, zoals deelname van de gemeente aan een rechtspersoon die voor de gemeente bepaalde diensten verricht;
3. De gegevensuitwisseling met derden;
4. De gegevensuitwisseling met derde partijen zoals bij samenwerkingsverbanden of leveranciers.

Wettelijk kader
Vanaf 25 mei 2018 is in de hele Europese Unie de Algemene verordening gegevensbescherming (AVG) van toepassing. Daar waar de AVG ruimte laat om op nationaal niveau bepaalde vraagstukken (aanvullend) te regelen, is dit in Nederland gedaan door middel van de Uitvoeringswet algemene verordening gegevensbescherming (UAVG). De UAVG is met ingang van 25 mei 2018 in werking getreden.

Daarnaast zijn er regels voor de verwerking van persoonsgegevens in het kader van de Wet politiegegevens (Wpg) en de Wet justitiële en strafvorderlijke gegevens (Wjsg). Deze wetten zijn het gevolg

van de implementatie van de EU-Richtlijn 2016/680. Voor zover de gemeente voornemens is een bestraffende sanctie op te leggen, valt de daarmee samenhangende verwerking van persoonsgegevens onder de reikwijdte van de Wpg. Een voorbeeld hiervan is de verwerking van persoonsgegevens door gemeentelijke BOA's.

Voor de bescherming van persoonsgegevens gelden de volgende wettelijke kaders:
- Algemene verordening gegevensbescherming (AVG);
- Uitvoeringswet algemene verordening gegevensbescherming (UAVG);
- Wet politiegegevens (Wpg);
- Archiefwet;
- Wet open overheid (Woo);
- Aanvullingen op dit algemene kader in sectorspecifieke wetten, zoals de Participatiewet, Jeugdwet en Wet basisregistratie personen.

Raakvlakken en overlap met andere beleidsthema's
Het privacybeleid kent raakvlakken met andere beleidsthema's of vertoont hiermee overlap. In dit verband wordt in het bijzonder genoemd:

Informatiebeveiliging
Informatiebeveiliging is van onmisbare waarde in de huidige digitale samenleving en vormt een randvoorwaarde voor de eerbiediging van de persoonlijke levenssfeer bij de verwerking van persoonsgegevens. In het 'Strategisch Informatiebeveiligingsbeleid 2023 en verder' van de gemeente Montfoort wordt op strategisch niveau het informatiebeveiligingsbeleid uiteengezet. Kernpunten hierbij zijn beschikbaarheid, integriteit en vertrouwelijkheid van persoonsgegevens en andere informatie.

Archiefbeleid
Het archiefbeleid is vastgelegd in de 'Beheerregeling informatiebeheer gemeente Montfoort 2019'. Hierin zijn bepalingen opgenomen over het ontvangen, creëren en uitwisselen van archiefbescheiden maar ook bepalingen over gegevensvernietiging. Deze voorschriften zijn gebaseerd op de Archiefwet.

Integriteit
Privacybewust werken en integer zijn raken elkaar. Integer zijn is niet voldoende om te voldoen aan de AVG, maar zorgvuldig omgaan met persoonsgegevens vereist een integere houding. In het kader van integriteit leggen nieuwe medewerkers de eed of belofte af en hebben zij een geheimhoudingsplicht.

Verantwoordelijkheid voor naleving AVG, Wpg en privacybeleid
Dit privacybeleid wordt centraal vastgesteld en is van toepassing op alle bestuursorganen van de gemeente; dit voor zover de AVG of Wpg op de betreffende verwerkingen van toepassing is.

Verantwoordelijkheid van iedere werknemer
Iedereen werkzaam binnen de gemeente is verantwoordelijk voor het verantwoord omgaan met persoonsgegevens. De gemeente verlangt van al haar medewerkers en alle personen die werkzaam zijn voor de gemeente dat de voorschriften van dit Privacybeleid worden opgevolgd en actief worden uitgedragen.

Het college B&W zal binnen de jaarlijkse planning & control cyclus de gemeenteraad informeren over de risico's en over de getroffen beheersmaatregelen op het gebied van privacy.

Privacy Officer (PO)
De PO is het interne aanspreekpunt voor wat betreft de praktische invulling van de vastgestelde privacy kaders en stemt voor zover nodig af met de FG. De hoofdtaken van de PO zijn:
- Adviseren over en meewerken aan het beleid/visie van de gemeente Montfoort op het gebied van privacy;
- Het bijhouden van wet- en regelgeving en jurisprudentie omtrent privacy;
- In samenwerking met CISO adviseren over de inrichting en veiligheid van de gegevensverwerkingen en de daarbij behorende datasystemen;
- Coördineren en adviseren bij het afhandelen van beveiligingsincidenten/datalekken conform de vastgestelde 'Procedure voor het melden van datalekken en beveiligingsincidenten'.

- Het melden van datalekken bij de Autoriteit Persoonsgegevens (AP).
- Bijhouden van het datalekkenregister;
- Het bewaken en borgen van de rechten van betrokkenen en de uitvoering van procedures die hiermee verband houden door proceseigenaren;
- Het bijdragen van bewustwording over het belang van privacy binnen de organisatie.

Een proceseigenaar is de medewerker die verantwoordelijkheid heeft ervoor te zorgen dat het proces aan de bedrijfsdoelstellingen blijft voldoen. Deze *medeweker draagt dus zorg voor een proces 'van klant tot klant' optimaal wordt uitgevoerd en, als het even kan, wordt verbeterd.*

Chief Information Security Officer (CISO)
De CISO is verantwoordelijk voor het implementeren van en toezicht houden op het Informatiebeveiligingsbeleid binnen de gemeente. De CISO heeft een centrale rol in het beheren van alle processen die daarmee te maken hebben en die moeten voldoen aan de BIO (Baseline Informatiebeveiliging Overheid); een set van organisatorische en technische beveiligingsmaatregelen die geïmplementeerd en beheerd dient te worden. De hoofdtaken van de CISO zijn:

- Het opstellen, bijstellen en vernieuwen van het informatiebeveiligingsbeleid;
- Het inrichten van de informatiebeveiligingsorganisatie;
- Het coördineren en adviseren bij afhandelen van beveiligingsincidenten conform de vastgestelde 'Procedure voor het melden van datalekken en beveiligingsincidenten'.
- Het toezien op naleving van de eigen voor informatiebeveiliging;
- Het bevorderen van het informatiebeveiligingsbewustzijn over de hele organisatie;
- Het adviseren bij en begeleiden van informatierisicoanalyses;
- Het uitvoeren van informatiebeveiliging assessments.

Functionaris Gegevensbescherming (FG)
Als overheidsinstantie verwerken wij structureel en op grote schaal (bijzondere) persoonsgegevens Daarom is er op grond van de AVG een FG aangesteld.

De FG is een onafhankelijke toezichthouder die gevraagd en ongevraagd advies geeft op het gebied van de AVG. De FG voert jaarlijks een interne audit uit en maakt daarbij een FG toezichtplan. De FG rapporteert jaarlijks over de naleving van privacy wet- en regelgeving aan het college van B&W. De FG heeft onder meer de volgende wettelijke taken:

- Toezicht op de implementatie en uitvoering van de privacy wet- en regelgeving;
- Adviseren en informeren over de AVG;
- Contactpersoon voor de Autoriteit Persoonsgegevens;
- Periodieke verslaglegging aan college van B&W over zijn bevindingen;
- Adviseren en beoordelen van uitgevoerde DPIA's;
- Informatie, adviezen en aanbevelingen geven.

Het is niet de bedoeling dat de FG de taken op het gebied van bescherming van persoonsgegevens van de proceseigenaren overneemt. De proceseigenaren hebben hun eigen verantwoordelijkheid in het juist verwerken van persoonsgegevens.

De FG heeft periodieke afstemming met de Privacy Officer (PO) en Chief Information Security Officer (CISO).

Uitgangspunten
De AVG omschrijft een aantal uitgangspunten die centraal staan in dit beleid. Hieronder worden deze uitgangspunten omschreven evenals de wijze waarop wij deze concreet invulling geven binnen onze organisatie.

Rechtmatigheid

- persoonsgegevens worden in overeenstemming met de geldende wet- en regelgeving verwerkt. Voor de verwerking van persoonsgegevens moet er altijd een wettelijke grondslag bestaan;
- persoonsgegevens worden alleen vastgelegd als dit noodzakelijk is voor het specifieke doel van verwerking;
- wij houden in het verwerkingsregister per verwerking bij op welke grondslag en met welk doel

deze verwerking gerechtvaardigd is;
- bij de gegevensverwerking wordt rekening gehouden met de beginselen van proportionaliteit en subsidiariteit. Dit betekent dat de inbreuk op de belangen van de betrokkene niet onevenredig mag zijn in verhouding tot en met de verwerking te dienen doel en dat voor het bereiken van het doel waarvoor de persoonsgegevens worden verwerkt, de inbreuk op de persoonlijke levenssfeer van de betrokken burger zoveel mogelijk wordt beperkt.

Behoorlijkheid
- wij hanteren het principe van 'minimale gegevensverwerking'. Dit betekent dat wij alleen de persoonsgegevens verwerken die minimaal noodzakelijk zijn voor het vooraf bepaalde doel;
- wij zorgen ervoor dat persoonsgegevens niet langer worden bewaard dan nodig is;
- in het geval van samenwerking met externe partijen waarbij sprake is van gegevensverwerking van persoonsgegevens, maken wij afspraken over gegevensuitwisseling en controleren wij of deze afspraken worden nageleefd;
- wij beschermen persoonsgegevens tegen ongeoorloofde toegang en nemen zowel technische als organisatorische maatregelen om persoonsgegevens te beschermen;
- wij zorgen door middel van workshops, trainingen en het op dagelijkse basis aandacht geven aan het belang van privacy bescherming ervoor dat onze medewerkers bewust zijn van het belang van privacy en dat in de praktijk zorg wordt gedragen voor de eerbiediging van de persoonlijke levenssfeer bij de verwerking van persoonsgegevens.

Transparantie
- inwoners hebben de mogelijkheid om te vragen welke persoonsgegevens wij van hen verwerken. In beginsel verstrekken wij de verzochte informatie, tenzij de wet anders aangeeft;
- om recht te doen aan verzoeken van burgers hebben wij een 'Procesbeschrijving – afhandeling AVG- en Wpg verzoeken' laten vaststellen. Hierin is beschreven op welke wijze verzoeken van betrokkenen door ons worden afgehandeld;
- wij houden een duidelijke en leesbare privacyverklaring bij die eenvoudig is te raadplegen;
- inwoners kunnen verzoeken om verbetering, aanvulling of verwijdering van persoonsgegevens doen. Er wordt naar gestreefd betrokkenen zoveel mogelijk zeggenschap te geven over hun gegevens. Betrokkenen kunnen gebruikmaken van hun rechten via een aanvraagformulier. De FG is tevens bereikbaar via (privacy@montfoort.nl).

Register van verwerkingen (art. 30 AVG)
Wij zijn verplicht tot het aanleggen van een register van alle verwerkingen van persoonsgegevens waarvan de gemeente de verwerkingsverantwoordelijke is. De volgende zaken worden vastgelegd in het register:
- de functionaris en de verwerkingsverantwoordelijke;
- de verwerkingsactiviteit;
- de doeleinden van de gegevensverwerking;
- een beschrijving van de categorieën van betrokkenen en van de categorieën van persoonsgegevens;
- een beschrijving van de categorieën van (voorgenomen) ontvangers;
- de grondslagen van verwerking;
- de beoogde bewaartermijnen.
- algemene beschrijving van de beveiligingsmaatregelen

Proceseigenaren melden nieuwe verwerkingen en relevante wijzigingen in bestaande verwerkingen aan de Privacy Officer. De Privacy Officer draagt er zorg voor dat deze nieuwe verwerkingen en relevante wijzigingen in het register opgenomen worden.

Datalekken
Incidenten zijn helaas niet in alle gevallen te voorkomen. Bij een datalek kan onder meer gedacht worden aan het kwijtraken van een USB stick met persoonsgegevens, het onbevoegd raadplegen van persoonsgegevens in een informatiesysteem, het aan iemand toesturen van een e-mailbericht met persoonsgegevens die niet voor de ontvanger bestemd is of het zoekraken van een dossier.

Een datalek kan potentieel een grote impact hebben.
Er worden daarom meerdere processen, systemen en acties ingezet om datalekken te voorkomen. Wij

spannen ons in voor het creëren van een cultuur waarin het snel melden van mogelijke datalekken worden gestimuleerd. Wij zijn wettelijk verplicht een datalek zonder onredelijke vertraging te melden bij de Autoriteit Persoonsgegevens, tenzij het niet waarschijnlijk is dat de inbreuk een risico inhoudt voor de rechten en vrijheden van natuurlijke personen.

Wij werken volgens de 'Procedure voor het melden van datalekken en beveiligingsincidentem'. Deze procedure is gericht op het snel en zorgvuldig kunnen afhandelen van incidenten. In de procedure staat beschreven op welke wijze datalekken worden afgehandeld en wie daarbij welke taken en verantwoordelijkheden heeft. Ook staat beschreven hoe en wanneer een datalek gemeld dient te worden bij de AP en/of betrokkenen. Daarnaast ontvangen onze medewerkers meerdere malen per jaar informatie over dit thema om de bewustwording op peil te houden.

Er wordt daarnaast een intern datalekkenregister bijgehouden waarin alle beveiligingsincidenten worden geregistreerd. Hierin wordt vastgelegd of het beveiligingsincident heeft geleid tot een datalek en indien dat het geval is, of het datalek ook is gemeld bij de AP en/of de betrokkenen. Jaarlijks wordt het datalekkenregister geëvalueerd om trends bij te houden en structurele verbeteringen intern door te voeren. Indien nodig worden datalekken direct geëvalueerd om zo dringende aanpassingen gelijk door te kunnen voeren in de organisatie.

DPIA (gegevensbeschermingeffectbeoordeling)
Voordat wij persoonsgegevens kunnen verwerken met een hoog privacy risico, zijn wij verplicht om een data protection impact assessment (DPIA) uit te voeren. Dit is een instrument om vooraf de privacyrisico's van een gegevensverwerking in kaart te brengen, zodat wij maatregelen kunnen nemen om deze risico's te verkleinen naar een minimaal en acceptabel niveau.

Wij hanteren een standaard DPIA model. Proceseigenaren zijn verantwoordelijk voor de uitvoering van een DPIA voor een verwerking met een hoog privacy risico. De PO ondersteunt en adviseert bij de uitvoering hiervan. De FG geeft advies over de uitgevoerde DPIA en ondertekent de DPIA. De uitgevoerde DPIA's worden bijgehouden in een register. De PO monitort de voortgang van het DPIA proces. Dit betekent dat de PO ongeveer een jaar na de uitgevoerde DPIA zal evalueren of de aanbevolen maatregelen zijn geïmplementeerd en of deze het gewenste effect behelzen. De PO informeert de FG over de bevindingen .

Processen kunnen regelmatig worden aangepast met mogelijke effecten op de verwerking. Als er een wijziging in het proces wordt doorgevoerd kan het noodzakelijk zijn om een eerder uitgevoerde DPIA te herzien en te kijken of de wijziging ook nieuwe risico's met zich meebrengt.

Inschakeling verwerkers, verwerkersovereenkomst
Verwerkers
De gemeente schakelt soms derden in om persoonsgegevens in opdracht van haar te verwerken. Deze derden worden verwerkers genoemd. Ook een verwerker moet zich houden aan de privacyregelgeving en aan het privacybeleid van de gemeente. De AVG verplicht gemeenten tot het maken van contractuele afspraken met verwerkers, zogenaamde verwerkersovereenkomsten.
De gemeente maakt gebruik van het format van de VNG. De PO ondersteunt en adviseert de proceseigenaar hierbij.

Camerabeelden
Camerabeelden binnen de gemeentelijke organisatie
De gemeente registreert op verschillende plekken (Huis van Montfoort en afvalscheidindingsstation, Gemeentewerf) bewegende beelden toe. Hiervoor geldt het 'Protocol cameratoezicht Huis van Montfoort en Afvalscheidingsstation Gemeentewerf'.

Privacy door ontwerp (privacy by design)
Bij het ontwerpen van producten en/of diensten, het inkopen van systemen en bij de uitvoering van haar werkzaamheden hanteert de gemeente de volgende uitganspunten hanteert:

Minimaal en gerechtvaardigd gebruik van persoonsgegevens:
- De gemeente verzamelt (of vraagt om) niet meer gegevens dan noodzakelijk of juridisch mogelijk;

- De gemeente verwerkt alleen gegevens voor het doel waarvoor zij zijn verzameld en verwerkt deze verder alleen op een manier die verenigbaar is met dit doel;
- Bij configuratie van systemen kiest de gemeente altijd voor de privacy-vriendelijke variant (privacy by default);
- De informatie die de gemeente verwerkt is correct en actueel;
- De gemeente maakt geen onnodige kopieën;
- De gemeente verwijdert wat niet meer nodig is.

Passende bescherming:

- De gemeente slaat gegevens zo op dat voldaan kan worden aan de wettelijke kaders van de AVG, dit betekent in verband met de doelbinding vaak gescheiden opslag;
- De gemeente beperkt de toegang tot inzage en wijzigen van gegevens tot degenen die dit vanuit hun functie nodig hebben;
- De gemeente beschermt persoonsgegevens door o.a. het aggregeren, versleutelen en anonimiseren van deze gegevens. Hierdoor wordt de mate waarin de verwerkte persoonsgegevens kunnen worden herleid verminderd.

Als uitgangspunt kiest de gemeente voor technische maatregelen om de privacy door ontwerp te waarborgen. Daar waar de technische mogelijkheden ontbreken of disproportioneel hoge kosten met zich meebrengen, zoekt de gemeente naar organisatorische en of procesmatige maatregelen als alternatief voor of als aanvulling op de technische maatregelen. Dit wordt uiteraard samen en in overleg met informatiebeveiliging uitgewerkt.

Privacy bij ontwerp dient organisatorisch geborgd te zijn om persoonsgegevens te kunnen beschermen. Binnen de gemeente worden vier relevante processen onderscheiden die zich bezighouden met het ontwerpproces van producten en diensten:

1. Demand-supply proces;
2. Architectuurproces;
3. Inkoopproces;
4. Contractproces.

Voor al deze vier de processen is het van belang om de PO en CISO te betrekken.

Rechten van betrokkenen

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

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

- recht op een menselijke blik bij besluiten/non profiling (artikel 22) : als op basis van automatisch verwerkte gegevens een besluit over iemand is genomen, kan iemand een nieuw besluit verlangen waar de gegevens door een mens worden beoordeeld.

Indienen van verzoek
Om gebruik te maken van deze rechten kan de betrokkene een verzoek indienen. De gemeente heeft vanaf ontvangst van het verzoek vier weken de tijd om een besluit te nemen op het verzoek. Wordt deze termijn overschreden, dan kan betrokkene de gemeente in gebreke stellen of een klacht indienen bij de FG. Voordat een verzoek in behandeling kan worden genomen, dient de identiteit van betrokkene vastgesteld te worden. Dit om fraude te voorkomen.

De gemeente voldoet aan het verzoek, tenzij er gerechtvaardigde gronden zijn om een verzoek af te wijzen. Een betrokkene heeft het recht om bezwaar te maken tegen de beslissing.

Beheer en onderhoud
Dit privacybeleid treedt in werking na vaststelling door het college van burgemeester en wethouders. Het beleid wordt eens in de vier jaar geëvalueerd en indien nodig herzien.
De FG wordt geïnformeerd op basis van deze evaluatie.

Inwerkingtreding en intrekking
Dit privacybeleid treedt in werking een dag na bekendmaking. Het Privacybeleid gemeente Montfoort, door het college vastgesteld op 8 mei 2018, en het Privacyreglement, door het college vastgesteld op 8 mei 2018, worden gelijktijdig met de inwerkingtreding van onderhavig privacy beleid ingetrokken.

Citeertitel
Dit beleid wordt aangehaald als: 'Privacybeleid gemeente Montfoort 2024'.

Aldus vastgesteld in de vergadering van burgemeester en wethouders van de gemeente Montfoort d.d. 27 februari 2024.

.....

M. H. van der Veer,
gemeentesecretaris

.....

mr. P.J. van Hartskamp-de Jong,
burgemeester