



Gegevensbeschermingseffectbeoordeling (DPIA)

Onderwerp : Salarisadministratie voor de gemeente Heemstede en Bloemendaal

Datum : 22 november 2022

Versie : 1.0

Inhoudsopgave

A. Beschrijving kenmerken gegevensverwerking	5
1. Voorstel.....	5
2. Persoonsgegevens	6
3. Gegevensverwerking	7
4. Verwerkingsdoeleinden	8
5. Betrokken partijen	10
6. Belangen bij de gegevensverwerking	11
7. Verwerkingslocaties.....	12
8. Technieken en methoden van de gegevensverwerking.....	13
9. Juridisch en beleidsmatig kader.....	14
10. Bewaartermijnen	15
B. Beoordeling rechtmatigheid gegevensverwerking.....	17
11. Rechtsgrond	17
12. Bijzondere persoonsgegevens	17
13. Doelbinding.....	18
14. Noodzaak en evenredigheid	19
15. Rechten van betrokkenen.....	21
C. Beschrijving en beoordeling risico's voor de betrokkenen	22
16. Risico's	22
D. Beschrijving voorgenomen maatregelen	23
17. Maatregelen	23
E. Eindafweging, conclusie en aanbevelingen	24

18. Eindafweging DPIA door CISO.....	24
19. Eindafweging DPIA door de FG.....	24
20. Conclusie en aanbevelingen	24
21. Handtekeningen.....	25
F. Bijlagen.....	26

A. Beschrijving kenmerken gegevensverwerking

1. Voorstel

Geef een korte introductie van de voorgenomen verwerking. Welke afdelingen zijn betrokken? Waarom wordt de verwerking overwogen? Wat is de achtergrond van de verwerking? Hoe is besloten om de voorgenomen verwerking eventueel in te gaan zetten?

De afdeling P&O voert de salarismutaties uit van het personeel van de gemeenten Heemstede en Bloemendaal. Deze kunnen onderverdeeld worden in twee categorieën: permanente mutaties en incidentele mutaties. Bij permanente mutaties kan worden gedacht aan het opvoeren van een nieuwe medewerker, het veranderen van het aantal uren van de arbeidsovereenkomst en het opvoeren van een vaste toelage. Incidentele mutaties betreffen veelal het uitbetalen van declaraties. Incidentele en permanente mutaties worden zowel op papier als digitaal aangeleverd.

De berekening, verwerking en uitbetaling van de salarissen vindt plaats in samenwerking met het bedrijf Visma-Raet. De salarisadministratie is verantwoordelijk voor de maandelijkse verwerking van salarissen.

2. Persoonsgegevens

Hieronder volgt een opsomming van de categorieën van persoonsgegevens die worden verwerkt. Per categorie van betrokkene is aangegeven welke persoonsgegevens van hem verwerkt worden. De persoonsgegevens zijn onderverdeeld in de volgende typen: gewoon, bijzonder, strafrechtelijke en wettelijk identificatienummer.

Categorie persoonsgegevens	Type en uitleg	Categorie betrokkenen
NAW-gegevens	Gewone gegevens	Medewerkers
BSN	Bijzonder gegeven	Medewerkers
Geboortedatum	Gewone gegevens	Medewerkers
Salarisgegevens en IKB	Gewone gegevens	Medewerkers
Verzuim- en verlofgegevens	Gewone gegevens	Medewerkers
Bankgegevens	Gewone gegevens	Medewerkers
Functiegegevens	Gewone gegevens	Medewerkers
Pensioengegevens	Gewone gegevens	Medewerkers
Ziektekostenverzekeraar	Gewone gegevens	Medewerkers

3. Gegevensverwerking

Hieronder wordt de voorgenomen gegevensverwerking weergegeven. Onder verwerking wordt verstaan: elke handeling, of elk geheel van handelingen met betrekking tot persoonsgegevens. Denk hierbij aan verzamelen, vastleggen, ordenen, structureren, opslaan, bewerken of wijzigen, opvragen, raadplegen, gebruiken, etc.

Mutaties worden op rechtmatigheid gecontroleerd en ingevoerd door de salarisadministrateurs. Zij controleren elkaars mutaties.

Visma Raet verwerkt de mutaties en levert de maandproductie op. De salarisadministrateur controleert deze op foutmeldingen en niet-verwerkte mutaties. De coördinator personeels- en salarisadministratie en de adviseur beheer P&O voeren ook nog een gedeeltelijke controle uit op de salarismutaties, bij het opstellen van het standenregister (een overzicht, waarin per medewerker en per afdeling een aansluiting wordt gemaakt tussen het bruto salaris van de huidige en de voorgaande maand; hierbij worden de mutaties 'medewerkers in en uit dienst', 'wijzigingen in de omvang van arbeidscontracten', 'algemene verhogingen' en 'periodieke verhogingen' in beeld gebracht). Deze controle betreft de vaste mutaties, zoals medewerkers nieuw in dienst en wijzigingen van arbeidsovereenkomsten.

Als alles akkoord is, worden de salarisspecificaties goedgekeurd en gepubliceerd in het medewerkersportaal Youforce van Visma-Raet. De betaling van de salarissen wordt geëxporteerd via een module van Visma Raet naar de applicatie van de Bank Nederlandse Gemeenten. De benodigde output wordt via de mail beschikbaar gesteld aan de financiële administratie, zodat zij de betalingen van de salarissen na goedkeuring van twee personen kunnen doorzetten. De medewerker financieel beheer zorgt voor de verantwoording van de salarissen in de financiële administratie. Financiën geeft met twee personen toestemming voor de uiteindelijke betaalbaarstelling. Loonaangifte en pensioenaangifte worden door de software aangemaakt en in een aparte module klaargezet. Salarisadministrateur geeft het akkoord en zorgt ervoor dat het geld naar de Belastingdienst en Pensioenfonds ABP gaat. De coördinator personeels- en salarisadministratie en de adviseur beheer P&O maken het standenregister. Het standenregister is een Excel-bestand dat op de afdelingsschijf staat en als het is opgesteld wordt het via YouForce aangeboden aan manager HRM facilitair waarna het wordt geaccordeerd.

De manier van verwerken van de gegevens staat uitgebreid uitgelegd in de 'Procesbeschrijving Salarisadministratie Gemeente Heemstede'. Deze is opgenomen in de bijlagen.

4. Verwerkingsdoeleinden

Hieronder worden de doeleinden beschreven van de voorgenomen gegevensverwerkingen.

Categorie persoonsgegevens	Verwerkingsdoeleinden	Oorsprong gegevens
NAW-gegevens	Om aan de juiste persoon salaris uit te betalen en de verplichtingen voor de Belastingdienst en Pensioenfonds klaar te zetten	Medewerker
BSN	Om de verplichtingen voor de Belastingdienst klaar te zetten	Medewerker
Geboortedatum	Dit gegevens is nodig voor het berekenen van het salaris.	Medewerker
Salarisgegevens	Om aan de juiste persoon salaris uit te betalen	Leidinggevende
Verzuim- en verlofgegevens	Verzuimgegevens worden verwerkt om bij ziekte het juiste salaris te kunnen betalen. Verlofgegevens worden verwerkt in het kader van aan- en verkoopverlof	Verzuim: leidinggevende Verlof: medewerker
Bankgegevens	Om het salaris op het juiste rekeningnummer te storten	Medewerker

Functiegegevens	Om het salarisoniveau te bepalen	Leidinggevende
Pensioengegevens	Om te zorgen voor correcte pensioenopbouw	Percentages komen vanuit de ABP
Ziektekostenverzekeraar	Om te zorgen voor correcte premiebetalingen	Bedragen komen van het IZA

5. Betrokken partijen

Hierna volgt een opsomming van de organisaties dan wel personen die betrokken zijn bij de gegevensverwerking en welke rol zij hebben: betrokkene, verwerkingsverantwoordelijke, verwerker, verstrekker of ontvanger. Ook is aangegeven welke functionarissen binnen deze organisaties toegang krijgen tot welke persoonsgegevens.

Betrokken partij	Rol	Functionaris	Toegang tot welke persoonsgegevens?
Betrokkene	Medewerker	Nvt	Toegang tot eigen gegevens in YouForce portaal
Verwerkingsverantwoordelijke	Het college	Manager HRM en Facilitair	Geen toegang
Verwerker	Visma Raet	Nvt	Indirect toegang tot alles
Verstrekker	Salarisadministrateur	Salarisadministrateur	Toegang tot alles
Ontvanger	Afdeling Financiën, Belastingdienst, ABP, IZA en medewerker	Afdeling Financiën: medewerker financieel beheer Belastingdienst ABP IZA Medewerker	Afdeling Financiën: salarisgegevens Belastingdienst: afdrachtgegevens ABP: premiegegevens IZA: premiegegevens Medewerker: eigen salarisgegevens

6. Belangen bij de gegevensverwerking

Hieronder staan de belangen beschreven die de verschillende partijen hebben bij de voorgenomen gegevensverwerkingen.

Betrokken partij	Belang
Medewerker	Juist en correct salaris, opbouw pensioen, afdracht loonheffing en zorgverzekering
Belastingdienst	Juiste betalingen loonheffingen
ABP	Juiste betaling pensioenpremie
IZA	Juiste betaling zorgverzekering

7. Verwerkingslocaties

De voorgenomen gegevensverwerking vindt plaats binnen de Europese Economische Ruimte (EER).

8. Technieken en methoden van de gegevensverwerking

Hierna volgt een beschrijving van de manier waarop en met gebruikmaking van welke (technische) middelen en methoden de persoonsgegevens worden verwerkt.

Techniek/methode	Noodzakelijkheid	Onderbouwing
Software en cloud Visma Raet	Noodzakelijk voor het correct verwerken van de geldelijke stromen	Noodzakelijk voor het correct verwerken van de geldelijke stromen

9. Juridisch en beleidsmatig kader

Hieronder is de voor deze gegevensverwerking relevante wet- en regelgeving (met uitzondering van de AVG en de Richtlijn) uitgewerkt, evenals het beleid met mogelijke gevolgen voor de voorgenomen gegevensverwerking.

Beschrijf hier elke relevante wet/verordening/beleid met de eventuele relevante artikelnummers, die op deze gegevensverwerking van toepassing zijn.

De Wet op de Loonbelasting, CAO Gemeenten, Gemeentewet, Personeelshandboek, Pensioenwet, APPA, Rechtspositie besluit decentrale politieke ambtsdragers en Regeling rechtspositie decentrale politieke ambtsdragers.

10. Bewaartermijnen

Categorie persoonsgegevens	Begin bewaartermijn	Termijn van bewaring	Motivatie bewaring	Verantwoordelijkheid voor verwijdering
NAW-gegevens	Na uitdiensttreding	7 jaar	Selectielijst gemeente	Proceseigenaar (gebeurt automatisch door het systeem)
Geboortedatum	Na uitdiensttreding	7 jaar	Selectielijst gemeente	Proceseigenaar (gebeurt automatisch door het systeem)
BSN	Na uitdiensttreding	7 jaar	Selectielijst gemeente	Proceseigenaar (gebeurt automatisch door het systeem)
Salarisgegevens	Na uitdiensttreding	7 jaar	Selectielijst gemeente	Proceseigenaar (gebeurt automatisch door het systeem)
Verzuimgegevens	Na ziekte	5 jaar	Selectielijst gemeente	Proceseigenaar (gebeurt automatisch door het systeem)
Verlofgegevens	Na uitdiensttreding	7 jaar	Selectielijst gemeente	Proceseigenaar (gebeurt automatisch door het systeem)
Bankgegevens	Na uitdiensttreding	7 jaar	Selectielijst gemeente	Proceseigenaar (gebeurt automatisch door het systeem)
Functiegegevens	Na uitdiensttreding	10 jaar	Selectielijst gemeente	Proceseigenaar (gebeurt automatisch door het systeem)
Pensioengegevens	Na uitdiensttreding	7 jaar	Selectielijst gemeente	Proceseigenaar (gebeurt automatisch door het systeem)

Ziektekostenverzekeraar	Na uitdiensttreding	7 jaar	Selectielijst gemeente	Proceseigenaar (gebeurt automatisch door het systeem)
-------------------------	---------------------	--------	------------------------	---

B. Beoordeling rechtmatigheid gegevensverwerking

11. Rechtsgrond

Neem hier een van de rechtsgronden uit de AVG op en werk deze uit. Het gaat daarbij om:

a. toestemming

b. uitvoering van een overeenkomst

c. wettelijke verplichting

d. vitaal belang van de betrokkene

e. algemeen belang/uitoefening openbaar gezag

f. gerechtvaardigd belang van de verantwoordelijke

Het is een wettelijke verplichting en een gerechtvaardigd belang van de verantwoordelijke.

12. Bijzondere persoonsgegevens

Categorie persoonsgegevens	Soort bijzonder persoonsgegeven	Noodzakelijkheid
BSN	Administratief nummer	Wettelijke verplichting
Pasfoto	Ras en geloof	Wettelijke verplichting via kopie paspoort

13. Doelbinding

De persoonsgegevens zullen niet voor een ander doel worden verwerkt dan oorspronkelijk verzameld.

14. Noodzaak en evenredigheid

Hierna volgt een beoordeling van de vraag of de voorgenomen gegevensverwerking noodzakelijk is voor het verwezenlijken van de verwerkingsdoeleinden. Aan de eisen van proportionaliteit en subsidiariteit wordt voldaan, zoals hieronder aangegeven.

- a. *proportionaliteit*: hierbij gaat het erom of de inbreuk op de persoonlijke levenssfeer en de bescherming van de persoonsgegevens van de betrokkenen in evenredige verhouding tot de verwerkingsdoeleinden staat.
- b. *subsidiariteit*: hierbij gaat het om de vraag of de verwerkingsdoeleinden in redelijkheid niet op een andere, voor de betrokkene minder nadelige manier, kunnen worden verwezenlijkt.

Categorie persoonsgegevens	Proportionaliteit	Subsidiariteit
NAW-gegevens	Ze zijn allemaal nodig voor de taken waarvoor ze worden verzameld.	Ze zijn allemaal nodig voor de taken waarvoor ze worden verzameld.
Geboortedatum	De geboortedatum is nodig voor de salarisadministratie.	De geboortedatum is nodig voor de salarisadministratie.
BSN	Dit is een wettelijke verplichting.	Dit is een wettelijke verplichting.
Salarisgegevens	Ze zijn allemaal nodig voor de taken waarvoor ze worden verzameld.	Ze zijn allemaal nodig voor de taken waarvoor ze worden verzameld.
Verzuim- en verlofgegevens	Ze zijn allemaal nodig voor de taken waarvoor ze worden verzameld.	Ze zijn allemaal nodig voor de taken waarvoor ze worden verzameld.
Bankgegevens	Zonder gegevens van de bank kan het salaris niet gestort worden.	Zonder gegevens van de bank kan het salaris niet gestort worden.

Functiegegevens	De functiegegevens zijn nodig om de medewerker het juiste salaris te kunnen geven.	De functiegegevens zijn nodig om de medewerker het juiste salaris te kunnen geven.
Pensioengegevens	De pensioengegevens zijn nodig voor de afdracht van de pensioenpremie en voor de opbouw van het pensioen.	De pensioengegevens zijn nodig voor de afdracht van de pensioenpremie en voor de opbouw van het pensioen.
Ziektekostenverzekeraar	De gegevens van de ziektekostenverzekeraar zijn nodig voor de afdracht van de ziektekostenpremie.	De gegevens van de ziektekostenverzekeraar zijn nodig voor de afdracht van de ziektekostenpremie.

15. Rechten van betrokkenen

Betrokkenen hebben op grond van de AVG rechten. Hierna volgt hoe daaraan invulling wordt gegeven.

Recht	Van toepassing? Mogelijk?	Hoe vindt informatieverstrekking aan betrokkene plaats?
Dataportabiliteit	n.v.t.	
Vergetelheid	n.v.t.	
Inzage	Ja, In de medewerkerskaart is een samenvatting te zien. Andere gegevens zijn deels op de loonstrook en bij het ABP in te zien.	
Rectificatie en aanvulling	Ja	Wordt bij de indiensttreding gemeld.
Beperking van de verwerking	N.v.t.	N.v.t.
Bezwaar tegen de verwerking	N.v.t.	N.v.t.
Informatie over de verwerking	Ja	Wordt bij de indiensttreding gemeld.

C. Beschrijving en beoordeling risico's voor de betrokkenen

In dit onderdeel wordt beschreven en beoordeeld wat de risico's van de voorgenomen gegevensverwerking zijn voor de rechten en vrijheden van de betrokkenen.

16. Risico's

Risico's en gevolgen	Oorsprong	Kans	Impact
Onrechtmatige toegang:	Laptop zonder schermbeveiliging laten staan; wachtwoord aan een ander geven	Klein	Zeer groot
Ongewenste wijziging:	Laptop zonder schermbeveiliging laten staan; wachtwoord aan een ander geven	Klein	Klein
Verloren gaan van gegevens:	Laptop zonder schermbeveiliging laten staan; wachtwoord aan een ander geven	Klein	Klein
Hack van de omgeving	Iemand dringt van buiten de systemen in;	Gemiddeld	Zeer groot

D. Beschrijving voorgenomen maatregelen

Er moeten maatregelen worden genomen om de hiervoor beschreven risico's van de voorgenomen gegevensverwerking voor de vrijheden en rechten van de betrokkenen aan te pakken.

17. Maatregelen

Risico's	Maatregel	Verantwoordelijke voor de maatregel	Prioriteit	Wanneer gereed?	Restrisico
Onrechtmatige toegang	Autorisaties, toegangsbeleid, bewustwording	Procesverantwoordelijke	-	Is al ingevoerd	Menselijk handelen
Ongewenste wijziging	Autorisaties, toegangsbeleid, bewustwording, vier-ogenprincipe en controles	Procesverantwoordelijke	-	Is al ingevoerd	Menselijk handelen
Verloren gaan van gegevens	Autorisaties, toegangsbeleid, bewustwording	Procesverantwoordelijke	-	Is al ingevoerd	Menselijk handelen
Hack van de gegevens	In het contract met de leverancier is opgenomen dat zij beveiligingsnormen moeten invoeren en hier rapportages over aanleveren.	Procesverantwoordelijke	-	Is opgenomen in de verwerkersovereenkomst	Menselijk handelen

E. Eindafweging, conclusie en aanbevelingen

18. Eindafweging DPIA door CISO

De risico's zijn afdoende afgedekt. Het grootste risico ligt bij de SaaS-leverancier. Zorg dat er goede contracten worden afgesloten, waarin informatiebeveiliging goed geadresseerd wordt en controles op informatiebeveiliging geleverd worden door de leverancier.

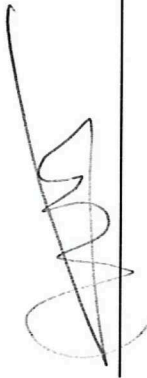
19. Eindafweging DPIA door de FG

	Akkoord	Niet akkoord	Opmerkingen
Grondslag	X		
Doelbinding	X		
Noodzakelijkheid	X		
Subsidiariteit en Proportionaliteit	X		

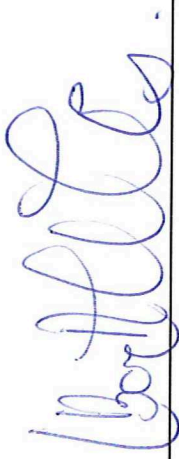
20. Conclusie en aanbevelingen

De verwerking voldoet aan de vereisten vanuit het oogpunt van informatiebeveiliging en privacy. Zorg dat er bij de aanschaf van nieuwe software goede contracten worden afgesloten, waarin informatiebeveiliging goed geadresseerd wordt en controles op informatiebeveiliging geleverd worden door de leverancier.

21. Handtekeningen



W. de Porto, CISO



U.M. Bouw-Althuisius, FG

Vastgesteld 1-12-2022



F. Bijlagen

1. Procesbeschrijving Salarisadministratie Gemeente Heemstede
2. Verwerkersovereenkomst met Visma Raet