

# Naleving en uitwerking AVG-plan afdeling Financiën 2023

## Inhoud

Naleving en uitwerking AVG-plan afdeling Financiën 2023 .....	1
Inleiding.....	2
Aanleiding en doel.....	2
Methode .....	2
Samenvatting.....	3
Verantwoording en naleving .....	4
Afdeling algemeen .....	4
Verduidelijking gebruik applicaties per proces.....	5
Nieuw financieel systeem (ERPx).....	6
Naleving DPIA Nieuw financieel systeem (ERPx).....	8
Belastingapplicatie GouwBelastingen .....	10
Naleving DPIA belastingapplicatie GouwBelastingen .....	11
Geautomatiseerde afhandeling No-Cure No-pay bezwaren.....	13
Naleving DPIA Geautomatiseerde afhandeling No-Cure No-pay bezwaren.....	14
Naleving DPIA SpendLab .....	15

# Inleiding

## Aanleiding en doel

Sinds 25 mei 2018 is de Algemene verordening gegevensbescherming (AVG) van toepassing. De AVG schrijft voor hoe organisaties om moeten gaan met het verzamelen, verwerken, opslaan en verwijderen van persoonsgevoelige informatie.

De volgende regels moeten worden gevolgd:

- **Transparantie:** de persoon van wie de gegevens verwerkt worden, is hiervan op de hoogte, heeft hiervoor toestemming gegeven en kent zijn rechten.
- **Doelbeperking:** de persoonsgegevens worden voor een welbepaald gewettigd doel verzameld, en mogen niet voor andere zaken gebruikt worden.
- **Gegevensbeperking:** enkel de gegevens die voor het beoogde doel noodzakelijk zijn, mogen worden verzameld.
- **Juistheid:** de persoonsgegevens moeten correct zijn en blijven.
- **Bewaarbeperking:** de persoonsgegevens mogen niet langer bewaard worden dan nodig voor het beoogde doel.
- **Integriteit en vertrouwelijkheid:** de persoonsgegevens moeten beschermd worden tegen toegang door onbevoegden, verlies of vernietiging.
- **Verantwoording:** de verantwoordelijke moet kunnen aantonen aan deze regels te voldoen.

De afdeling Financiën verwerkt persoonsgegevens in diverse systemen, de belangrijkste zijn GouwIT en Unit4 Financials (CODA). Deze gegevens zijn nodig voor het garanderen van de rechtmatigheid en juistheid van de financiële boekhouding. De afgelopen jaren is er steeds meer aandacht voor de vertrouwelijkheid van informatie en de maatregelen die nodig zijn om veilig te handelen. Er wordt steekproefsgewijs gekeken hoe de verschillende bureaus ermee omgaan, maar een volledig overzicht van welke gevoelige informatie de afdeling precies heeft en hoe er mee om wordt gegaan, ontbreekt. Daarom is gevraagd om een verkennend onderzoek, om dit voor de afdeling in beeld te brengen.

## Doel

Met dit onderzoek willen we verder *in control* komen op het gebied van AVG op de afdeling: we willen weten bij welke processen en/of organisatieonderdelen er binnen Financiën gebruik gemaakt wordt van verschillende persoonsgevoelige gegevens (*zie Afdeling Algemeen*), hoe daar mee om wordt gegaan, wat onzekerheden en risico's zijn en hoe we met deze risico's om moeten of willen gaan (risicobereidheid). Om zo meer inzicht en grip te krijgen op de AVG bij Financiën en te kunnen bepalen welke vervolgstappen er nodig zijn om de afdeling verder AVG-proof te krijgen. Hierbij is gekeken naar gebruikte systemen, processen en gegevens (op hoofdlijnen) en naar welk gedrag en bewustzijn daarvoor nodig is onder medewerkers.

Daarnaast draagt dit onderzoek bij aan de jaarlijkse verantwoording van de stand van zaken rond de AVG binnen Financiën, aan de Functionaris Gegevensbescherming (FG). De afgelopen jaren is de rol van de Functionaris Gegevensbescherming (FG) en de Privacy Officer (PO) steeds meer vormgegeven in de organisatie. Zij hebben een controlerende (FG) en adviserende (PO) rol wat betreft de waarborging van de vertrouwelijkheid van persoonsgegevens.

## Methode

In januari 2020 is het AVG-implementatieplan opgesteld voor de afdeling Financiën. Voorafgaand heeft er een inventarisatie plaatsgevonden binnen alle bureaus. Gedurende het afgelopen jaar is er uitvoering gegeven aan het implementatieplan. Hierbij is vooral aandacht besteed aan het creëren van bewustwording van alle medewerkers binnen Financiën.

# Samenvatting

De afdeling Financiën maakt op meerdere plekken gebruik van persoonsgegevens. Zoals bij inhuur van medewerkers, heffen van belastingen en leges en het uitkeren van subsidies. Aan het verwerken van gegevens zitten grofweg twee elementen. Ten eerste het inregelen van veilige systemen, autorisaties en de afspraken daaromheen. Ten tweede het gedrag van medewerkers: wordt er aan afspraken gehouden, zijn medewerkers zich bewust van AVG en hun rol daarin?

Zoals genoemd werkt de afdeling Financiën in de huidige situatie met het systeem Unit4 Financials (Coda), echter gaan we in 2024 een nieuw financieel systeem implementeren genaamd ERPx, ontwikkeld door Unit4. Dit biedt ons de uitgelezen kans om de processen nog beter AVG-proof te maken. Dit is gedaan door een adviesgroep op te richten onder de naam 'AVG & Archivering' waarbij de betrokkenen verantwoordelijk zijn voor het toezien op een goede naleving van de AVG en bijkomende privacyrechten in het nieuwe financiële systeem. Daarnaast is de DPIA voor het nieuwe financieel systeem (FIS 2024) in februari 2023 goedgekeurd door de Functionaris Gegevensbescherming. Tevens is de verwerkersovereenkomst opgesteld en getekend door beiden partijen. De naleving op de DPIA's en de verwerkersovereenkomst valt verder te lezen in dit verslag.

Voor zowel het inregelen van veilige systemen als voor gedrag is de indruk dat er rekening gehouden wordt met AVG en dat de afgelopen jaren de nodige maatregelen zijn getroffen. Daarmee lijkt Financiën een heel eind op weg te zijn en in zekere mate *in control* te zijn. Wel is er een aantal maatregelen dat genomen kan/moet worden en blijft het nodig om in de bureaus af en toe stil te staan bij AVG. Een datalek of onjuist gebruik van persoonsgegevens zit in een klein hoekje. Daarnaast blijft het altijd zoeken naar de balans tussen risico's volledig afdekken (bv. slechts één of twee personen ergens toegang toe geven) en het werkbaar houden (bv. elkaar kunnen vervangen bij uitval). Algemene afdrank is dat we goed op weg zijn maar het blijft mensenwerk.

# Verantwoording en naleving

## Afdeling algemeen

Financiën	
<b>Globale stand van zaken</b>	Binnen de afdeling Financiën heerst de indruk dat er afgelopen jaren meer aandacht en bewustzijn voor de AVG is gekomen en dat er verschillende verbeterlagen zijn gedaan. Deze indrukken zijn op basis van opgeleverde DPIA's en verwerkersovereenkomsten, het in het leven roepen van een adviesgroep 'AVG & Archivering' binnen de implementatie van het nieuwe financiële systeem (ERPx), het aanstellen van privacy ambassadeurs en het faciliteren van trainingen op het gebied van de AVG. Maar ook overige acties zoals het verder beschermen van persoonsgegevens door het opslaan van fysieke documenten in een kast, achter slot en grendel. We merken dat o.a. bij inkoop er meer bewustwording is ontstaan over het verwerken van privacygevoelige informatie doordat de privacy-ambassadeurs steeds meer vragen krijgen over de verwerking van informatie op inkoopfacturen. Ten slotte zijn veel problemen met datalekken de afgelopen jaren niet voorgekomen.
<b>Systemen totaal</b>	<ul style="list-style-type: none"><li>- Allegro</li><li>- Amis</li><li>- Beaufort/Gemal</li><li>- CityPermit</li><li>- Cognos</li><li>- Corsa</li><li>- Crescendo</li><li>- Energiemissie</li><li>- E-verbinding</li><li>- GBA</li><li>- Gouw IT</li><li>- GWS</li><li>- Key2Betalen</li><li>- Key2Data</li><li>- Key2Subsidie</li><li>- Lias</li><li>- LTC</li><li>- MBVO</li><li>- Planon</li><li>- Power2Pay</li><li>- SG Treasury</li><li>- Tableau</li><li>- Totallink</li><li>- VSA Kassa</li></ul>
<b>Belangrijkste risico's</b>	<ul style="list-style-type: none"><li>- Toegang tot persoonsgegevens is niet beperkt in applicaties die gebruikt worden bij de afdeling Financiën (zie systemen totaal);</li><li>- Er is geen grondslag om persoonsgegevens binnen applicaties te verwerken;</li><li>- De verwerking van persoonsgegevens is niet gebonden aan specifieke verzameldoelen;</li><li>- Autorisaties binnen applicaties die gebruikt worden bij de afdeling Financiën voor toegang tot persoonsgegevens zijn niet juist ingericht;</li><li>- Persoonsgegevens worden langer bewaard dan nodig;</li><li>- De rechten van betrokkenen zijn niet goed ingericht/nageleefd in de financiële processen;</li><li>- Er worden binnen de applicaties die gebruikt worden bij de afdeling Financiën meer persoonsgegevens verstrekt dan gewenst;</li></ul>
<b>Uitgangspunten acties afdeling algemeen i.r.t. AVG-proof 2024</b>	<ul style="list-style-type: none"><li>- De financiële applicaties worden (opnieuw) ingericht op basis van een autorisatiestructuur. Functioneel beheer kan deze autorisaties zonder tussenkomst van de opdrachtnemer instellen/wijzigen/verwijderen. Dit moet ook in bulk mogelijk zijn.</li></ul>

	<ul style="list-style-type: none"> <li>- Wanneer er persoonsgegevens verwerkt worden in een financiële applicatie wordt een DPIA opgesteld waarin de processen met bijbehorende grondslagen beschreven zijn. Indien in het vervolg blijkt dat er een proces bijkomt, zal de DPIA aangepast en uitgebreid moeten worden. Mocht vervolgens blijken dat we ons niet kunnen berusten op een grondslag, dan moet het proces aangepast worden.</li> <li>- De bewaartermijnen uit de geldende Selectielijst gemeentelijke en intergemeentelijke organen 2020 worden toegepast. De Gemeentelijke Selectielijsten zijn op grond van de Archiefwet vastgesteld (<a href="https://vng.nl/sites/default/files/2020-02/selectielijst_20200214.pdf">https://vng.nl/sites/default/files/2020-02/selectielijst_20200214.pdf</a>.)</li> <li>- Meer afwegen mogelijkheden tot pseudonimiseren en/of anonimiseren van persoonsgegevens bij het gebruik ervan. Dit onderdeel maken van het proces rond bewustwording AVG en omgang met persoonsgegevens.</li> </ul>
--	---

### Verduidelijking gebruik applicaties per proces

Proces	Applicaties
Inkoop inclusief betalen	Corsa E-verbinding Power2Pay
Verkoop inclusief incasseren en aanmanen	Planon MBVO LTC
Uitbetaling buiten het inkoopproces	Energiemissie GWS CityPermit Key2Subsidie Allegro
Relatiebeheer	Key2Data GBA
Journaliseren	CityPermit Gouw IT GWS SG Treasury Amis Key2Betalen Key2Subsidie Allegro VSA Kassa Crescendo Beaufort
Rapporteren	Cognos Tableau Lias Totallink

	<b>Nieuw financieel systeem (ERPx)</b>
Globale stand van zaken	<p>Binnen het nieuw financieel systeem (ERPx) verwerkt onze gemeente persoonsgegevens ten behoeve van een correcte verwerking en voeren van een juiste financiële administratie. Om hier zorg voor te dragen is de adviesgroep 'AVG &amp; Archivering' opgericht waarin de projectleden zich bezighouden met AVG-gerelateerde kwesties en helpen om het systeem AVG-proof in te richten. Daarnaast is het nieuw financieel systeem (ERPx) goedgekeurd ter gebruik als archiefsysteem. Dit oordeel is tot stand gekomen door bovenstaande adviesgroep en in samenwerking met Unit4, Bureau Documentaire Informatievoorziening (BDI, Gemeente Nijmegen) en archiefinspecteur <sup>5.1.2e</sup> (Gemeente Nijmegen).</p> <p>Dit oordeel zorgt ervoor dat er geen koppeling meer nodig is met Corsa en betekent dat Financiën, functioneel beheer, goed moet inrichten omdat Bureau Documentaire Informatievoorziening op deze manier niet meer verantwoordelijk is. Wat nu extra aandacht vergt is de concrete implementatie en borging van de punten die van belang zijn rond AVG &amp; Archivering zoals opgenomen in het programma van eisen. Hieronder volgt de verdere uitwerking en verantwoording.</p> <p>Er is onderscheidt gemaakt in de specificatie van de te nog nemen acties door de adviesgroep AVG &amp; Archivering, zoals in dit hoofdstuk beschreven en voortkomend uit de werkzaamheden van de adviesgroep AVG &amp; Archivering. Daarnaast is de verdere verantwoording op de risicoanalyse en daarop te nemen maatregelen, vanuit de eerder opgestelde DPIA, in volgend hoofdstuk benoemd.</p>
Belangrijkste risico's	<ul style="list-style-type: none"> <li>- Toegang tot persoonsgegevens is niet beperkt in ERPx</li> <li>- Er is geen grondslag om persoonsgegevens binnen ERPx te verwerken;</li> <li>- De verwerking van persoonsgegevens is niet gebonden aan specifieke verzameldoelen binnen ERPx</li> <li>- Autorisaties binnen ERPx zijn niet goed ingericht</li> <li>- Persoonsgegevens worden langer bewaard dan nodig binnen ERPx</li> <li>- De rechten van betrokkenen zijn niet goed ingericht/nageleefd in de financiële processen;</li> <li>- Er worden binnen het gebruik van ERPx meer persoonsgegevens verstrekt dan gewenst;</li> </ul>

<p>Acties opgesteld door de adviesgroep AVG &amp; Archivering 2024</p>	<ul style="list-style-type: none"> <li>- Er moet een lijst met vereiste essentiële/noodzakelijke/minimale metadata per archiefbescheiden (dossiers/documenten/bestanden) worden opgesteld;</li> <li>- Er moet een lijst van toegestane invoer per metadata worden opgesteld. Uitwerking in de vorm van keuzelijsten of standaardinvoerwaarden;</li> <li>- Opstellen en vaststellen van bewaartermijnen voor archiefbescheiden (dossiers/documenten/bestanden) aan de hand van geregistreerde metadata en/of landelijke selectielijst;</li> <li>- Opstellen van een lijst van stamgegevens of in te voeren boekingsgegevens/journaalposten waarbij een bijlage verplicht is;</li> <li>- Het via procedures vaststellen en genereren van vernietigingslijsten op basis van verlopen bewaartermijn en zorg dragen voor daadwerkelijke vernietiging;</li> <li>- Het via procedures vaststellen en zorg dragen dat metadata t.a.t. gekoppeld blijft aan het dossier, ook bij migraties van dossiers;</li> <li>- Opstellen van een lijst van stamgegevens of in te voeren boekingsgegevens/journaalposten waarbij een bijlage verplicht is;</li> <li>- Toekennen en vastleggen van autorisaties in de zin van gebruikersrollen, om rechten te beschermen en onjuiste toegang te voorkomen. Dit naar functies, processen en afdelingen van gebruikers.;</li> <li>- Procedureel inrichten dat betrokkenen hun rechten kunnen uitoefenen (inzage, wijzigen, verwijderen van gegevens etc.);</li> <li>- Het genereren van rapportages en exports dient procedureel te zijn ingericht;</li> <li>- Er moet aangesloten worden op de procedure jaarlijkse digitale vernietiging van BDI;</li> <li>- Opstellen van een lijst van informatie over waar de papieren documenten (als die binnenkomen) worden gescand en hoe deze onder een aanvullend vervangingsbesluit kunnen vallen (dus dat de papieren originelen vernietigd mogen worden);</li> </ul>
<p>Borging en verantwoording</p>	<ul style="list-style-type: none"> <li>- Bovenstaande acties worden meegenomen in de implementatie van ERPx en bij de training van de betrokken functioneel beheerders;</li> <li>- Het financieel proces is opgenomen in het register van verwerkingen. Dit register is openbaar te raadplegen;</li> <li>- Er is een verwerkersovereenkomst opgesteld en getekend door beide partijen;</li> <li>- Het nieuw financieel systeem werkt op basis van een autorisatiestructuur en functioneel beheer en kan deze autorisaties zonder tussenkomst van de opdrachtnemer instellen/wijzigen/verwijderen;</li> <li>- in de DPIA zijn de processen met bijbehorende grondslagen beschreven. Deze zijn tevens goedgekeurd door de Functionaris Gegevensbescherming;</li> <li>- De bewaartermijnen uit de geldende Selectielijst gemeentelijke en intergemeentelijke organen 2020 worden toegepast. De Gemeentelijke Selectielijsten zijn op grond van de Archiefwet vastgesteld;</li> <li>- De verplichtingmakers krijgen de verantwoordelijkheid om de incidentele bijzondere persoonsgegevens te verwijderen of te herzien in verplichtingregels. Dit afgestemd worden met het MT-financiën. De instructies worden opgenomen in concrete werkinstructies en de verplichtingmakers krijgen hiervoor een training. De crediteurenadministratie krijgt verdere instructie (werkinstructie en fysieke training) over hoe te handelen indien zij (bijzondere)-persoonsgegevens signaleren op een inkoopfactuur;</li> </ul>

## Naleving DPIA Nieuw financieel systeem (ERPx)

<b>Risico's:</b>	<b>Maatregel(en):</b>	<b>Verantwoording:</b>
<i>Autorisaties voor de toegang tot persoonsgegevens zijn niet juist ingericht.</i>	<i>Het nieuw financieel systeem werkt op basis van een autorisatiestructuur en functioneel beheer en kan deze autorisaties zonder tussenkomst van de opdrachtnemer instellen/wijzigen/verwijderen. Dit moet ook in bulk mogelijk zijn.</i>	<i>Er wordt gezorgd dat het nieuw financieel systeem werkt op basis van een autorisatiestructuur. Dit is meegenomen in het programma van eisen (PvE) en zal bij de verdere inrichting van het nieuw financieel systeem worden meegenomen. De huidige situatie is dat we nog niet in de situatie zijn om deze stap te gaan nemen binnen de implementatie, maar deze staat wel op de planning voor 2024. Functioneel beheer zal hierbij betrokken zijn in samenspraak met de adviesgroep AVG &amp; Archivering.</i>
<i>Autorisaties voor de toegang tot persoonsgegevens worden niet op een juiste manier toegepast/nageleefd.</i>	<i>Gebruikersrechten en -rollen worden centraal door de functioneel beheerder toebedeeld, gecontroleerd en gewijzigd (rolebased acces). Deze controle vindt minimaal één keer per maand plaats. Er worden daarnaast logbestanden bijgehouden, waarin staat wie welke wijziging heeft doorgevoerd en welke gebruikers de acties hebben uitgevoerd en op welke gegevens de aanpassingen betrekking hebben. Op basis van deze informatie kan functioneel beheer zonder tussenkomst van de opdrachtnemer, autorisaties instellen/wijzigen/verwijderen.</i>	<i>Voor de verantwoording geldt hetzelfde als de verantwoording beschreven bij bovenstaand risico.</i>
<i>De verwerking van persoonsgegevens is niet gebonden aan specifieke verzameldoelen.</i>	<i>In de DPIA zijn de processen met bijbehorende grondslagen beschreven. Indien blijkt dat er een proces bijkomt, zal de DPIA aangepast en uitgebreid moeten worden. Mocht vervolgens blijken dat we ons niet kunnen berusten op een grondslag, dan moet het proces aangepast worden.</i>	<i>In de DPIA zijn de processen met bijbehorende grondslagen beschreven. Er blijkt tot op heden geen proces te zijn bijgekomen, waardoor de DPIA ook niet uitgebreid hoeft te worden.</i>
<i>Persoonsgegevens worden langer bewaard dan nodig.</i>	<i>De bewaartermijnen uit de geldende Selectielijst gemeentelijke en intergemeentelijke organen 2020 worden toegepast. De Gemeentelijke Selectielijsten zijn op grond van de Archiefwet vastgesteld</i>	<i>De bewaartermijnen uit de geldende Selectielijst gemeentelijke en intergemeentelijke organen 2020 worden toegepast.</i>

	<a href="https://vng.nl/sites/default/files/2020-02/selectielijst_20200214.pdf">https://vng.nl/sites/default/files/2020-02/selectielijst_20200214.pdf</a> .	
<i>Er zijn onvoldoende contractuele afspraken gemaakt.</i>	<i>In het opstellen en naleven van de contractuele afspraken zal extra aandacht gaan naar de volgende onderdelen: software-functionaliteit, AVG-compliance, beveiliging van persoonsgegevens, beschikbaarheid van persoonsgegevens &amp; garanties en aansprakelijkheid.</i>	<i>De volgende contracten zijn opgesteld: SaaS-contract en verwerkersovereenkomst.</i>
<i>De SaaS provider gaat failliet.</i>	<i>De SaaS provider voorziet in de waarborging van de continuïteit van het nieuwe financieel systeem zoals beschreven in de GIBIT 2020 art. 30.2 iii</i>	<i>Er zijn geen indicatoren die suggereren dat dit het geval is, maar de afspraken over continuïteit zijn opgenomen in het SaaS-contract.</i>
<i>Er is geen procedure over hoe we om gaan met verzoeken van betrokkenen.</i>	<i>De gekozen leverancier van het nieuwe financieel systeem, levert documentatie waarin staat beschreven welke privacy-maatregelen door hen zijn genomen. Deze documentatie wordt ook opgeleverd als onderdeel van de verwerkersovereenkomst. Daarnaast wordt het nieuwe financieel systeem 'privacy-by-design' ingericht. Dit is opgenomen in het programma van eisen (PvE) in de aanbesteding.</i>	<i>De adviesgroep AVG &amp; Archivering heeft beoordeeld dat het nieuwe financieel systeem 'privacy-by-design' is ingericht. Ook voldoet ERPx aan de eisen zoals die gesteld zijn in het programma van eisen, als onderdeel van de aanbesteding. Er is documentatie waaruit dit blijkt en kan opgevraagd worden bij de adviesgroep AVG &amp; Archivering.</i>
<i>Bij het beoordelen van verzoeken van betrokkenen bestaat het risico dat er een verkeerde beslissing genomen wordt.</i>	<i>Bij het beoordelen van verzoeken van betrokkenen bestaat het risico dat er een verkeerde beslissing genomen wordt.</i>	<i>In 2024 wordt er een werkinstructie opgesteld.</i>
<i>Bijzondere persoonsgegevens worden (per ongeluk) opgenomen in de facturen of boekingsregels van het nieuwe financieel systeem.</i>	<i>De verplichtingmakers krijgen de verantwoordelijkheid om de incidentele bijzondere persoonsgegevens te verwijderen of te herzien in verplichtingregels. Dit wordt afgestemd met het MT-financiën. De instructies worden opgenomen in concrete werkinstructies en de verplichtingmakers krijgen hiervoor een training. De crediteurenadministratie krijgt verdere instructie (werkinstructie en fysieke training) over hoe te handelen indien zij (bijzondere)-persoonsgegevens signaleren op een inkoopfactuur.</i>	<i>De maatregel, zoals hiernaast beschreven, wordt in 2024 verder opgepakt.</i>

	<b>Belastingapplicatie GouwBelastingen</b>
Globale stand van zaken	<p>De belastingapplicatie van GouwIT ondersteunt jaarlijks bij het opleggen en innen van aanslagen gemeentelijke belastingen. Daarnaast het registreren van objecten (gebouwde en ongebouwde eigendommen) en subjecten (natuurlijke en niet-natuurlijke personen gegevens).</p> <p>Deze gegevensverwerking is noodzakelijk om de hoogte van de belasting te kunnen bepalen en de juiste belastingplichtigen een aanslag gemeentelijke belastingen op te kunnen leggen en de administratie te voeren ten behoeve van heffing en inning van gemeentelijke belastingen.</p> <p>Gemeenten Nijmegen komt een ruime vrijheid toe bij het vertalen van hun beleid in belastingverordeningen. Zo heeft ook gemeente Nijmegen de vrijheid om in haar politieke besluitvorming de heffingsmaatstaf, de hoogte van het tarief en de tariefdifferentiatie vast te stellen. Die beleidsvrijheid is echter niet onbegrensd en mag bijvoorbeeld niet in strijd zijn met algemene rechtsbeginselen.</p> <p>Er is sprake van stelselmatige monitoring en structureel observeren van de gegevens. De gegevens worden maandelijks gecontroleerd op juistheid, volledigheid voordat deze gebruikt worden. Daarnaast vindt er achteraf een controle plaats, in de vorm van interne controle, van de gebruikte gegevens.</p> <p>Op 31 december 2022 is de samenwerking met het printbureau Paragon beëindigd. Vanaf 1 januari 2023 is er, na een aanbesteding, een contract met DataB afgesloten.</p>
Belangrijkste risico's	<ul style="list-style-type: none"> <li>- Datalekken of privacy-inbreuken bij leverancier GouwIT;</li> <li>- Certificering beveiliging van gegevens, controle door derden;</li> <li>- Afspraken en structureel overleg over beheer, beveiliging van gegevens en autorisatie tussen de gemeente Nijmegen en GouwIT;</li> <li>- Onderzoek door de kwaliteitsmedewerker, tweemaal per jaar, naar de autorisaties binnen het Gouw-systeem;</li> <li>- Datalekken of privacy- inbreuken bij Cannock Chase;</li> <li>- Certificering beveiliging van gegevens, controle door derden;</li> <li>- Jaarlijks brengt Cannock Chase een ISAE3402 Type II assurance rapport uit;</li> <li>- Structureel overleg tussen de gemeente Nijmegen en Cannock Chase over beheer en beveiliging van gegevens en de voortgang;</li> <li>- Datalekken of privacy- inbreuken bij Paragon;</li> <li>- Certificering beveiliging van gegevens, controle door derden;</li> <li>- Jaarlijks brengt Paragon een ISAE3402 Type II assurance rapport uit;</li> <li>- Structureel overleg tussen de gemeente Nijmegen en Paragon over beheer en beveiliging van gegevens en de voortgang;</li> </ul>
Te nemen acties	<ul style="list-style-type: none"> <li>- Gelet op de beschreven maatregelen die al genomen zijn in het kader van informatiebeveiliging en privacybescherming en de constatering dat deze tot nu toe goed functioneren, is er geen aanleiding om aanvullende maatregelen te treffen.</li> </ul>
Borging en verantwoording	<ul style="list-style-type: none"> <li>- De beschreven risico's worden in voldoende mate geborgd en op een juiste wijze verantwoord.</li> </ul>

## Naleving DPIA belastingapplicatie GouwBelastingen

Als onderdeel van het controleplan FG 2022 is er binnen de afdeling Financiën verdere invulling gegeven aan de DPIA van de belastingapplicatie GouwBelastingen. Hierbij is gekeken in hoeverre de eerder beschreven risico's en bijpassende maatregelen gedurende de uitvoering van dit project, gehandhaafd worden. Om een beeld te scheppen zijn hieronder de risico's en maatregelen inclusief argumentatie voor de afdeling Financiën verder beschreven.

<b>Risico's:</b>	<b>Maatregel(en):</b>	<b>Verantwoording:</b>
<i>Datalekken of privacy-inbreuken bij leverancier GouwIT</i>	<i>Bij de softwareleverancier GouwIT zijn beveiligingsmaatregelen genomen in de belastingapplicatie.</i>	<i>Tot nu toe zijn er geen datalekken bij de leverancier GouwIT bekend of andere privacy-inbreuken aan het licht gekomen. Met GouwIT is een verwerkingsovereenkomst afgesloten.</i>
<i>Certificering beveiliging van gegevens, controle door derden</i>	<i>De beveiliging van gegevens door derden gecontroleerd en gecertificeerd.</i>	<i>Het certificaat ISAE 3402 type II is afgegeven door Conclude Accountants.</i>
<i>Afspraken en structureel overleg over beheer, beveiliging van gegevens tussen de gemeente Nijmegen en GouwIT</i>	<i>De afspraken over beheer, beveiliging en performance worden verantwoord in een Service Level Rapportage (SLR)</i>	<i>Maandelijks wordt er door GouwIT aan de gemeente Nijmegen een Service Level Rapportage (SLR) toegestuurd.</i>
<i>Onderzoek door de kwaliteitsmedewerker van de autorisaties</i>	<i>De kwaliteitsmedewerker voert tweemaal per jaar een onderzoek uit naar de autorisaties binnen de Gouw-applicatie.</i>	<i>De kwaliteitsmedewerker stelt tweemaal per een rapportage op van de uitgevoerde onderzoeken en stuurt deze rapportage naar de manager Gemeentebelastingen.</i>
<i>Er vindt een datalek plaats</i>	<i>Er worden zo min mogelijk gevoelige gegevens verstrekt om de gevolgen van een datalek te beperken. De eerder vastgestelde bewaartermijn wordt gehanteerd zodat gegevens niet langer bewaard worden dan nodig.</i>	<i>Afgelopen jaar is er een datalek geconstateerd en doorgegeven aan de manager en de CISO. Het datalek is geanalyseerd en opgelost. Conclusie was dat er adequaat gehandeld is en verdere maatregelen niet nodig waren.</i>
<i>Datalekken of privacy- inbreuken bij Cannock Chase</i>	<i>Bij het externe incasso bureau Cannock Chase zijn beveiligingsmaatregelen genomen in hun applicatie.</i>	<i>Tot nu toe zijn er geen datalekken bij de leverancier Cannock Chase bekend of andere privacy-inbreuken aan het licht gekomen. Met Cannock Chase is een verwerkingsovereenkomst afgesloten.</i>
<i>Certificering beveiliging van gegevens, controle door derden</i>	<i>De beveiliging van gegevens door derden gecontroleerd en gecertificeerd.</i>	<i>Cannock Chase heeft een ISO 27001 certificering voor hun IT processen.</i>

<i>Jaarlijks brengt Cannock Chase een ISAE3402 Type II assurance rapport uit</i>	<i>De afspraken over beheer, beveiliging en performance worden verantwoord in een ISAE3402 Type II assurance rapport.</i>	<i>Cannock Chase heeft een ISAE3402 Type II assurance rapport.</i>
<i>Structureel overleg tussen de gemeente Nijmegen en Cannock Chase over beheer en beveiliging van gegevens en de voortgang</i>	<i>De afspraken over beheer, beveiliging en performance worden verantwoord in een</i>	<i>Jaarlijks worden twee evaluatiegesprekken gepland met Cannock Chase waarbij de resultaten, doorlooptijden, voortgang en actuele ontwikkelingen op invorderingsgebied besproken wordt.</i>
<i>Datalekken of privacy- inbreuken bij DataB</i>	<i>Bij het printbedrijf DataB zijn beveiligingsmaatregelen genomen in hun applicatie.</i>	<i>Tot nu toe zijn er geen datalekken bij de leverancier Pragon bekend of andere privacy-inbreuken aan het licht gekomen. Met DataB is een verwerkingsovereenkomst afgesloten.</i>
<i>Certificering beveiliging van gegevens, controle door derden</i>	<i>De beveiliging van gegevens door derden gecontroleerd en gecertificeerd.</i>	<i>DataB heeft een ISO 14001- en OHSAS 18001 certificaat.</i>
<i>Jaarlijks brengt DataB een ISAE3402 Type II assurance rapport uit</i>	<i>Rapport ISAE3402 Type II assurance.</i>	<i>DataB heeft een ISAE3402 Type II assurance rapport.</i>
<i>Structureel overleg tussen de gemeente Nijmegen en Cannock Chase over beheer en beveiliging van gegevens en de voortgang</i>	<i>De afspraken over beheer, beveiliging en performance worden verantwoord in een</i>	<i>Jaarlijks vindt er tussen de gemeente Nijmegen en DataB plaats. Dit overleg gaat over de evaluatie, voortgang en de planning.</i>

	<b>Geautomatiseerde afhandeling No-Cure No-pay bezwaren</b>
Globale stand van zaken	<ul style="list-style-type: none"> <li>- Het automatiseren van bezwaren van No-Cure No-Pay bedrijven, die namens belastingplichtige bezwaar tegen de aanslag gemeentelijke belastingen. Het is gebruikelijk dat er om een hoorzitting en onderbouwende informatie wordt gevraagd. De opgevraagde gegevens dienen wettelijk gezien, verplicht aan dit soort bedrijven worden toegezonden.</li> <li>- Het doel is het afhandelen van bezwaarschriften WOZ. De huidige wijze is niet duurzaam om te doen want de huidige werkwijze is inefficiënt en te kostbaar. Het automatiseren van een deel van het werkproces zorgt dat het proces efficiënter en effectiever uitgevoerd kan worden, daarnaast levert het een kostenbesparing op.</li> <li>- Door de manager Gemeentebelasting is een kosten batenanalyse gemaakt van dit werkproces waarbij ook is gekeken naar effectiviteit en efficiency. Het niet of onjuist verstrekken van incomplete of onjuiste informatie brengt voor de gemeente Nijmegen financiële risico's, in de vorm van proceskosten veroordeling bij de Rechtbank met zich mee.</li> <li>- Het afgelopen jaar heeft het geautomatiseerd afhandelen van No-Cure No-pay bedrijven veel tijdsbesparing opgeleverd. Daarnaast is dit proces veel efficiënter en effectiever uitgevoerd waardoor er een kostenbesparing is geweest.</li> </ul>
Belangrijkste risico's	<ul style="list-style-type: none"> <li>- Datalekken of privacy-inbreuken bij leverancier GouwIT;</li> <li>- Certificering beveiliging van gegevens, controle door derden;</li> <li>- Afspraken en structureel overleg over beheer, beveiliging van gegevens en autorisatie tussen de gemeente Nijmegen en GouwIT;</li> <li>- Onderzoek door de kwaliteitsmedewerker, tweemaal per jaar, van de autorisaties binnen het Gouw-systeem;</li> </ul>
Te nemen acties	<ul style="list-style-type: none"> <li>- Gelet op de beschreven maatregelen die al genomen zijn in het kader van informatiebeveiliging en privacybescherming en de constatering dat deze tot nu toe goed functioneren, is er geen aanleiding om aanvullende maatregelen te treffen.</li> </ul>
Borging en verantwoording	<ul style="list-style-type: none"> <li>- De beschreven risico's worden in voldoende mate geborgd en op een juiste wijze verantwoord.</li> </ul>

## Naleving DPIA Geautomatiseerde afhandeling No-Cure No-pay bezwaren

Als onderdeel van het controleplan FG 2022 is er binnen de afdeling Financiën verdere invulling gegeven aan de DPIA van de belastingapplicatie GouwBelastingen. Hierbij is gekeken in hoeverre de eerder beschreven risico's en bijpassende maatregelen gedurende de uitvoering van dit project, gehandhaafd worden. Om een beeld te scheppen zijn hieronder de risico's en maatregelen inclusief argumentatie voor de afdeling Financiën verder beschreven.

<b>Risico's:</b>	<b>Maatregel(en):</b>	<b>Verantwoording:</b>
<i>Datalekken of privacy-inbreuken bij leverancier GouwIT</i>	<i>Bij de softwareleverancier GouwIT zijn beveiligingsmaatregelen genomen in de belastingapplicatie.</i>	<i>Tot nu toe zijn er geen datalekken bij de leverancier GouwIT bekend of andere privacy-inbreuken aan het licht gekomen. Met GouwIT is een verwerkingsovereenkomst afgesloten.</i>
<i>Certificering beveiliging van gegevens, controle door derden</i>	<i>De beveiliging van gegevens door derden gecontroleerd en gecertificeerd.</i>	<i>Het certificaat ISAE 3402 type II is afgegeven door Conclude Accountants.</i>
<i>Afspraken en structureel overleg over beheer, beveiliging van gegevens tussen de gemeente Nijmegen en GouwIT</i>	<i>De afspraken over beheer, beveiliging en performance worden verantwoord in een Service Level Rapportage (SLR)</i>	<i>Maandelijks wordt er door GouwIT aan de gemeente Nijmegen een Service Level Rapportage (SLR) toegestuurd.</i>
<i>Onderzoek door de kwaliteitsmedewerker van de autorisaties</i>	<i>De kwaliteitsmedewerker voert tweemaal per jaar een onderzoek uit naar de autorisaties binnen de Gouw-applicatie.</i>	<i>De kwaliteitsmedewerker stelt tweemaal per een rapportage op van de uitgevoerde onderzoeken en stuurt deze rapportage naar de manager Gemeentebelastingen.</i>

## Naleving DPIA SpendLab

Als onderdeel van het controlplan FG 2022 is er binnen de afdeling Financiën verdere invulling gegeven aan de DPIA van Spendlab. Hierbij is gekeken in hoeverre de eerder beschreven risico's en bijpassende maatregelen gedurende de uitvoering van dit project, gehandhaafd worden. Om een beeld te scheppen zijn hieronder de risico's en maatregelen inclusief argumentatie voor de afdeling Financiën verder beschreven.

<b>Risico's:</b>	<b>Maatregel(en):</b>	<b>Verantwoording:</b>
<i>Toegang tot gegevens is niet beperkt</i>	<i>Alleen bevoegde personen aan de kant van SpendLab hebben toegang tot de gegevens (personen die aan dit project zijn gekoppeld, dit zijn 2 of 3 personen). Het restrisico dat overblijft is het risico dat de bevoegde personen misbruik maken van de gegevens.</i>	<i>De consultants van SpendLab hebben de inhoudelijke visuele analyse alleen ter plaatse uitgevoerd in Nijmegen, onder toezicht van een medewerker van gemeente Nijmegen. Hierbij is één Citrix account uitgedeeld met raadpleegfunctie tot Coda.</i>
<i>Er worden meer persoonsgegevens verstrekt dan gewenst</i>	<i>De enige persoonsgegevens die verstrekt worden aan SpendLab zijn de boekingsomschrijvingen en elementnamen (waar voor-en achternamen in kunnen voorkomen). Dit dient vooraf aan de uitwisseling van data gecontroleerd te worden door de gemeente Nijmegen. Het restrisico dat overblijft is dat na controle kan blijken dat er toch meer persoonsgegevens in de dataset zitten. Deze gegevens worden vervolgens verwijderd.</i>	<i>De boekingsomschrijvingen en elementnamen zijn de enige objecten die persoonsgegevens kunnen bevatten. Deze zijn vooraf steekproefsgewijs bekeken door een medewerker van de gemeente Nijmegen.</i>
<i>Er vindt een datalek plaats</i>	<i>Er worden zo min mogelijk gevoelige gegevens verstrekt om de gevolgen van een datalek te beperken. De eerder vastgestelde bewaartermijn wordt gehanteerd zodat gegevens niet langer bewaard worden dan nodig. Dataset wordt aangeleverd via mSafe. SpendLab is ISO27001 gecertificeerd en voldoet aan de daaraan gestelde beveiligingseisen.</i>  <i>Dataset is aangeleverd via mSafe. SpendLab is tevens ISO27001 gecertificeerd en voldoet aan de daaraan gestelde beveiligingseisen.</i>	<i>In december 2022 is er een aanvraag gedaan naar SpendLab ter verantwoording van het gebruik van een minimale gegeven set en verwijdering van gegevens die niet meer noodzakelijk zijn. Vanuit SpendLab ontvingen wij het antwoord dat het destijds nog te vroeg was voor het elimineren van de data. Zie de verantwoording hieronder voor een vervolg daarop.</i>
<i>De gegevens worden langer bewaard dan vooraf vastgesteld</i>	<i>Gemeente Nijmegen ziet toe op naleving van de bewaartermijn door SpendLab. Dit zal tussentijds als aan het einde van het project gecontroleerd worden.</i>	<i>Het project zit in een afrondende fase omdat er een definitief resultaat is bereikt. Data van gemeente Nijmegen kan dus verwijderd worden aan de kant van SpendLab. Dit verzoek is bij SpendLab uitgezet. SpendLab zal</i>

		<p>intern zorg dragen voor eliminering van de data, daar hebben wij een bevestiging van ontvangen. Voor wat betreft de definitieve eliminering en het resultaat daarvan: daar ontvangen wij nog een bevestiging van. Het is onze taak om toe te zien op de eisen opgesteld in de verwerkersovereenkomst. 5.1.2e 5.1.2e en 5.1.2e zien hierop toe wanneer het project definitief is afgerond.</p>
--	--	--

# Legenda toegepaste uitzonderingsgrondslagen

In dit document zijn gegevens geanonimiseerd op grond van:

Wet	Artikel	Omschrijving	Pagina's
Wet open overheid	Art. 5.1 lid 2 sub e	De eerbiediging van de persoonlijke levenssfeer	6, 16