

Uitwerking AVG-plan afdeling Financiën

Inhoud

Uitwerking AVG-plan afdeling Financiën.....	1
Inleiding.....	2
Aanleiding en doel.....	2
Methode	2
Samenvatting.....	3

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 daarom heen. 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 loopt er op dit moment een aanbesteding voor een nieuw financieel systeem. Dit biedt ons de uitgelezen kans om de processen nog beter AVG-proof te maken. De DPIA voor de nieuwe situatie ligt ter beoordeling en advies bij de Functionaris Gegevensbescherming.

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).

Afdeling algemeen	
Globale stand van zaken	<i>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 faciliteren van trainingen op het gebied van de AVG en overige genomen acties (zie bevindingen). Veel problemen met datalekken zijn de afgelopen jaren overigens niet voorgekomen.</i>
Systemen totaal	<ul style="list-style-type: none"> - Corsa - E-verbinding - Power2Pay - Planon - MBVO - LTC - Energiemissie - GWS - CityPermit - Key2Subsidie - Allegro - Key2Data - GBA - CityPermit - Gouw IT - GWS - SG Treasury - Amis - Key2Betalen - Key2Subsidie - Allegro - VSA Kassa - Crescendo - Beaufort - Cognos - Tableau - Lias - Totallink
Belangrijkste risico's	<ul style="list-style-type: none"> - Toegang tot persoonsgegevens is niet beperkt in applicaties die gebruikt worden bij de afdeling Financiën; - Er is geen grondslag om persoonsgegevens binnen applicaties te verwerken; - De verwerking van persoonsgegevens is niet gebonden aan specifieke verzameldoelen; - Autorisaties binnen applicaties die gebruikt worden bij de afdeling Financiën voor toegang tot persoonsgegevens zijn niet juist ingericht; - Persoonsgegevens worden langer bewaard dan nodig; - De rechten van betrokkenen zijn niet goed ingericht/nageleefd in de financiële processen; - Er worden binnen de applicaties die gebruikt worden bij de afdeling Financiën meer persoonsgegevens verstrekt dan gewenst;
Mogelijke acties	<ul style="list-style-type: none"> - 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. - 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. - De bewaartermijnen uit de geldende Selectielijst gemeentelijke en intergemeentelijke organen 2020 worden toegepast. De Gemeentelijke Selectielijsten zijn op grond van de

	<p>Archiefwet vastgesteld (https://vng.nl/sites/default/files/2020-02/selectielijst_20200214.pdf.)</p> <ul style="list-style-type: none"> - Afwegen mogelijkheden tot pseudonimiseren en/of anonimiseren van persoonsgegevens bij het gebruik ervan;
Al uitgevoerde acties	<ul style="list-style-type: none"> - In 2022 zijn er voor de medewerkers van de afdeling Financiën een aantal bijeenkomsten georganiseerd om aan de verplichte StudyTube trainingen te werken. Specifiek de trainingen op het gebied van privacy, informatiebeheer en informatiebeveiliging. Deze bijeenkomsten zijn drie keer gehouden met een tijdsduur van 120 minuten. Medewerkers hadden zelf de mogelijkheid om aan te sluiten. - De fysieke kast op de eerste verdieping stadhuis (bij crediteuren) is op slot gezet. Hierdoor is het niet zo maar meer mogelijk om fysieke facturen te bekijken. De medewerkers die hier wel toegang voor nodig hebben, hebben een sleutel. - Voor de afdeling Financiën is “de week van de AVG” (mei, 2022) gehouden. Hierbij is op maandag tot en met vrijdag een onderwerp op het gebied van de AVG verder toegelicht via iNsite. Elke dag werd er tevens een Poll gedeeld via iNsite met een vraag over het desbetreffende onderdeel. Als naslagwerk zijn er twee posters gemaakt (AVG, wat moeten we ermee ?!) & (DPIA binnen de AVG). De posters zijn ook gedeeld op iNsite. Er is tevens vernomen dat de posters ook bij een andere afdeling in gebruik zijn genomen. - De DPIA voor SpendLab is gemaakt en goedgekeurd door de Functionaris Gegevensbescherming (Peter Kluver). Daarnaast is de DPIA voor het nieuwe financieel systeem (FIS 2024) in de maak. De eerste (concept)versie is eind december gedeeld met de Privacy Officer (5.1.2e) en de Functionaris Gegevensbescherming. In januari 2023 is de DPIA ontvangen en voorzien van feedback vanuit de Privacy Officer. De feedback is verwerkt en de DPIA is inmiddels met de Functionaris Gegevensbescherming gedeeld. - Begin december 2022 zijn er door bureau belastingen, twee DPIA's ingediend bij de Functionaris Gegevensbescherming. Dit zijn de DPIA's voor gemeentebelastingen (incl. belastingapplicatie Gouw) & Digitale afhandeling No Cure No Pay. Deze DPIA's zijn goedgekeurd door de Functionaris Gegevensbescherming. Deze DPIA's vallen in de control-cyclus van 2023. - De werkprocessen van het bureau Gemeentebelastingen zijn AVG-proof ingericht. Met de externe bedrijven, Data B, Cannock Chase, Legitiem en GouwIT zijn verwerkingsovereenkomsten afgesloten en voldoen aan de eisen. Bureau Gemeentebelastingen voldoet hiermee aan de eisen van de AVG.

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.

Risico's:	Maatregel(en):	Verantwoording:
Toegang tot gegevens is niet beperkt	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.	De consultants van SpendLab mochten de inhoudelijke visuele analyse alleen ter plaatse uitvoeren in Nijmegen, onder toezicht van een medewerker van gemeente Nijmegen. Hierbij is één Citrix account uitgedeeld met raadpleegfunctie tot Coda.

<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>Er is een uitvraag gedaan naar SpendLab ter verantwoording van het gebruik van een minimale gegeven set en verwijdering van gegevens die niet meer noodzakelijk zijn. Aangezien het project nog loopt, is verwijdering van gegevens aan het einde van het project nog niet aan de orde. Dataset is aangeleverd via mSafe. SpendLab is tevens ISO27001 gecertificeerd en voldoet aan de daaraan gestelde beveiligingseisen.</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>Er is een uitvraag gedaan naar SpendLab voor een statusupdate rond de verwijdering van gegevens die niet meer noodzakelijk zijn.</i>

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	5