Raadsmededeling openbaar

Nummer	:	122-2024
Datum		30 juli 2024
B&W datum	:	2 juli 2024
Beh. Ambtenaar	:	Anky Bruil
Portefeuillehouder	:	mr. A.B. Stapelkamp
Onderwerp	:	Rapportage toetsing AVG 2023

Aanleiding:

Elk jaar vindt er een interne toetsing plaats in het kader van de Algemene Verordening Gegevensbescherming (AVG). Deze wordt uitgevoerd door de Functionaris Gegevensbescherming. Door middel van deze interne toetsing krijgen we een beeld in hoeverre de AVG binnen onze organisatie wordt nageleefd.

Inhoud mededeling:

Sinds 2018 is de Algemene Verordening Gegevensbescherming (AVG) van kracht die tot doelstelling heeft om de privacy en persoonsgegevens van burgers te beschermen. Onze Functionaris Gegevensbescherming ziet toe op de naleving en toepassing van de AVG. Hierover rapporteert zij jaarlijks aan het College van Burgemeesters en Wethouders. Door middel van de interne toetsing krijgen we een beeld in hoeverre wij voldoen aan de AVG binnen onze gemeente en waar verbeteringen nodig zijn. De rapportage is gebaseerd op de vragenlijst van de Informatiebeveiligingsdienst, het ‘AVG Borgingsproduct 3.0’. De vragen in het borgingsdocument zijn geactualiseerd ten opzichte van 2022. Zo zijn bijvoorbeeld maatregelen verduidelijkt en in sommige gevallen samengevoegd. De vragenlijst is ingevuld samen met de privacy coördinator en vormt een omvangrijk Excel document. Om die reden is een infographic gemaakt, met een beeldende weergave van de toetsingsresultaten.

In de bijlage ‘Digitale Weerbaarheid Aalten 2023’ (bijlage 1) geeft de Functionaris Gegevensbescherming een overzicht van de stand van zaken met betrekking tot de implementatie van de verschillende thema’s van de AVG. Per thema is aangegeven welke onderwerpen in 2024 (verder) kunnen worden uitgewerkt om steeds meer aan de AVG te voldoen. Een groot deel van het risico op incidenten rondom privacy en informatiebeveiliging wordt veroorzaakt door menselijk handelen. Bewustwording van onze medewerkers blijft daarom ook voor 2024 een belangrijk aandachtspunt. Om ons volwassenheidsniveau op het gebied van de AVG te verhogen heeft de Functionaris Gegevensbescherming diverse aanbevelingen gedaan. We nemen deze aanbevelingen op in een actieplan Privacy. De aanbevelingen worden geprioriteerd en de belangrijkste aanbevelingen worden opgenomen in het Informatieveiligheidsplan Gemeente Aalten 2024.

De volgende stukken zijn voor u bijgevoegd:

‘Digitale weerbaarheid, bekeken vanuit de AVG 2023’

HET TIJD-PERK VAN

Digitale weerbaarheid

Bekeken vanuit de AVG

2023

Gemeente Aalten



56% Samenwerking
Richt het leveranciersmanagement in

81% Beleid
Uitdragen beleid
Opnemen acceptatie restrisico's

69% Processen
Inregelen logging
Overzicht van werkprocessen
Wens AVG-certificering
Vul enkele processen aan
Breng hoog risico verwerkingen in beeld

69% Rechten van betrokkenen
Toevoeging formulier
Inrichten klantportaal
Aansluiten algoritmeregister
Aanvullen privacyverklaring met geautomatiseerde besluitvorming
Publicatie register van verwerkingen

46% Verantwoording
Inrichten ISMS/PIMS
Inzicht management
Meer toetsingen
Evalueer beleid, procedure en proces

70% Gegevensbescherming
Aanvullen crisis(communicatie) voor datalekken
Inbedden handleiding privacy by design
Leer van fouten
Inrichten PDCA cyclus in ISMS/PIMS

73% Organisatorische inbedding
Opstellen bewustwordingsprogramma
Meer menskracht AI en Wpg
Aanwijzen FG alle bestuursorganen
Aanvullen arbeidsovereenkomst

PRIVACY

Informatie is een levensader van de organisatie. Als digitale overheid is het daarom belangrijk om digitaal weerbaar te zijn.

Blijf leren hoe u veilig kunt omgaan met persoonsgegevens, zodat inwoners niet in de knel komen en u een betrouwbare overheid bent.

Om privacy verder vorm te geven zijn de begrippen bewustwording en sturing essentieel.

Blijf medewerkers bewust maken van zowel bestaande onderwerpen als van nieuwe ontwikkelingen zoals algoritmes en kunstmatige intelligentie. Zorg daarnaast voor voldoende inzicht in deze onderwerpen bij het management zodat sturing mogelijk is.

Uitleg toetsing

Met behulp van het toetsingsdocument 'AVG Borgingsproduct 3.0' van de IBD heb ik als FG op diverse thema's (witte tekst) een toets uitgevoerd. Per thema is aangegeven welke onderwerpen in 2024 (verder) kunnen worden uitgewerkt om steeds meer aan de AVG te voldoen. Het volledige borgingsdocument is bekend bij de privacycoördinator van uw organisatie. De onderwerpen die het meest bijdragen aan verbetering staan aangegeven als focusgebied voor 2024.

Focusgebieden 2024

- Logging
- ISMS/PIMS
- Werk-processen

10
Datalekken zijn gemeld bij de privacy coördinator

1
Datalek is gemeld bij de Autoriteit Persoonsgegevens

1
Datalek is gemeld aan betrokkene(n)

MT-besluit gemeente Aalten

Zaakkenmerk/Onderwerp	Z/24/149986/Toetsing AVG 2023
Verantwoordelijk organisatieonderdeel	A4 Team Informatiebeheer
Zaakkenmerk/Documentkenmerk	Z/24/149986/D-522345
Vertrouwelijkheid	Openbaar

Toelichting voorstel

Samenvatting

Portefeuillehouder: Burgemeester A.B. Stapelkamp

Sinds 2018 is de Algemene Verordening Gegevensbescherming (AVG) van kracht die tot doelstelling heeft om de privacy en persoonsgegevens van burgers te beschermen. Onze Functionaris Gegevensbescherming ziet toe op de naleving en toepassing van de AVG. Hierover rapporteert zij jaarlijks aan het College van Burgemeesters en Wethouders. Door middel van de interne toetsing krijgen we een beeld in hoeverre wij voldoen aan de AVG binnen onze gemeente en waar verbeteringen nodig zijn. De rapportage is gebaseerd op de vragenlijst van de Informatiebeveiligingsdienst, het 'AVG Borgingsproduct 3.0'. De vragen in het borgingsdocument zijn geactualiseerd ten opzichte van 2022. Zo zijn bijvoorbeeld maatregelen verduidelijkt en in sommige gevallen samengevoegd. De vragenlijst is ingevuld samen met de privacy coördinator en vormt een omvangrijk Excel document. Om die reden is een infographic gemaakt, met een beeldende weergave van de toetsingsresultaten.

Voorgestelde beslispunten

Beslispunten:

1. Kennis te nemen van de interne toetsing AVG 2023 aan de hand van de infographic "Digitale weerbaarheid bekeken vanuit de AVG 2023" (bijlage 1).
2. In te stemmen met de rapportage interne toetsing AVG 2023 en de benodigde actiepunten.
3. De raad met een raadsmededeling te informeren over de uitkomsten van de interne toetsing AVG 2023

Besluit

Akkoord.

Inleiding

Sinds 2018 is de AVG-wetgeving van kracht die tot doelstelling heeft om de privacy en persoonsgegevens van burgers te beschermen. Onze Functionaris Gegevensbescherming ziet toe op de naleving en toepassing van de AVG. Hierover rapporteert zij jaarlijks aan het College van Burgemeesters en Wethouders. Door middel van de interne toetsing krijgen we een beeld in hoeverre de AVG binnen onze gemeente wordt nageleefd. De rapportage is gebaseerd op de vragenlijst van de Informatiebeveiligingsdienst, het 'AVG Borgingsproduct 3.0'. De vragenlijst is ingevuld samen met de privacy coördinator en vormt een omvangrijk Excel document. Om die reden is een infographic gemaakt, met een beeldende weergave van de toetsingsresultaten.
In de bijlage 'Digitale Weerbaarheid Aalten 2023' (bijlage 1) geeft de Functionaris Gegevensbescherming een overzicht van de stand van zaken met betrekking tot de implementatie van de verschillende thema's van de AVG. Per thema is aangegeven welke onderwerpen in 2024 (verder) kunnen worden uitgewerkt om steeds meer aan de AVG te

voldoen. Een groot deel van het risico op incidenten rondom privacy en informatiebeveiliging wordt veroorzaakt door menselijk handelen. Bewustwording van onze medewerkers blijft daarom ook voor 2024 een belangrijk aandachtspunt. Om ons volwassenheidsniveau op het gebied van de AVG te verhogen heeft de Functionaris Gegevensbescherming diverse aanbevelingen gedaan. We nemen deze aanbevelingen op in een actieplan Privacy. De aanbevelingen worden geprioriteerd en de belangrijkste aanbevelingen worden opgenomen in het Informatieveiligheidsplan Gemeente Aalten.

De Functionaris Gegevensbescherming adviseert de volgende focusgebieden voor 2024:

- Logging
- ISMS/PIMS (Information/Privacy Security Management System)
- Werkprocessen

Deze focusgebieden zijn terug te vinden in de volgende onderwerpen en aanbevelingen die dan ook van belang zijn:

Processen:

- Inregelen logging
- Overzicht van werkprocessen
- Wens AVG-certificering
- Vul processen aan
- Breng hoog risicoverwerkingen in beeld

Verantwoording:

- Inrichten ISMS/PIMS
- Inzicht management
- Meer toetsingen
- Evalueer, beleid, procedure en proces

De percentages in de Infographic van de Functionaris Gegevensbescherming geven een indicatie van in welke mate we voldoen aan het (landelijk) normenstelsel met betrekking tot de implementatie van de AVG. We krijgen zo inzicht in hoeverre we als gemeente voldoen aan de wetgeving met betrekking tot het veilig en zorgvuldig verwerken van de persoonsgegevens van onze burgers. Dit is echter geen garantie op veiligheid van de privacy met betrekking tot de persoonsgegevens die onder de verantwoordelijkheid van de gemeente vallen. We proberen wel elk jaar weer een stapje te maken in de AVG-volwassenheid van onze organisatie.

Argumenten

De percentages geven een beeld in hoeverre we de AVG ingebed hebben in onze organisatie. We zetten steeds stapjes vooruit in de ontwikkeling en inbedding van de AVG. In vergelijking met de andere gemeenten in onze samenwerking doen we het op bepaalde onderdelen goed en op bepaalde onderdelen wat minder. Op de onderdelen beleid en organisatorische inbedding doen we het goed. Het valt op dat het onderdeel “Verantwoording” achterblijft en verbetert moet worden. Dit heeft dan ook prioriteit. Onder “Verantwoording” verstaan we het verbeteren van de evaluatie van de naleving van de AVG. Er moet meer periodiek getoetst worden op beleid, naleven van processen en procedures. Ook is het van belang dat, bij de uitvoering van de taken van het management, de naleving van de AVG geëvalueerd wordt. Om dit beter te organiseren zijn we in 2023 begonnen met het in brengen van de processen en applicaties waarin persoonsgegevens worden verwerkt, in een speciaal ontwikkelde ISMS/PMS, namelijk Pepperflow GRC (Governance, Risk, Compliance). Het inbrengen van de processen stagneert echter doordat Pepperflow GRC niet voldoet aan de wensen vanuit privacy. Pepperflow is bezig de applicatie te optimaliseren. Hier moeten we in 2024 stappen zetten om het onderdeel “Verantwoording” te verbeteren.

Ook moeten we werkprocessen vastleggen. Zo krijgen we een goed beeld van waar de persoonsgegevens worden verwerkt binnen de gemeente. Dit is dan ook een belangrijke aanbeveling. De AVG ziet toe op het verantwoord verwerken van de persoonsgegevens. Dit kan alleen goed als we de werkprocessen goed in beeld hebben gebracht.

Logging is van belang in het kader van de transparantie. In de AVG gaat het om transparantie. In dat kader moeten wij kaders/beleid hebben op het gebied van logging.

Om privacy in de organisatie goed in te bedden is het ook van belang dat we samenwerken vanaf de start van een nieuw idee, project of proces. Zo kunnen we groeien in ons volwassenheidsniveau en ontstaat een organisatie die weet wat ze met de persoonsgegevens doet, hier transparant over is en betrouwbaar is naar haar inwoners, medewerkers en (samenwerkings) partners.

Bewustwording blijft één van de belangrijkste maatregelen tegen beveiligingsincidenten en datalekken. Het is de basis voor zorgvuldige omgang met persoonsgegevens. We moeten dan ook structureel aandacht besteden aan de risico's en hoe zorgvuldig om te gaan met de persoonsgegevens van onze inwoners en medewerkers.

Kanttekeningen

We hebben geen onbeperkte middelen en mensen om alle voorgestelde aanbevelingen direct aan te kunnen pakken. We gaan de aanbevelingen prioriteren en de belangrijkste aanbevelingen nemen we op in het Informatieveiligheidsplan. Het inbrengen van de processen in Pepperflow GRC heeft prioriteit maar vergt veel tijd. Er zijn meerdere jaren nodig om dit te realiseren.

Overleg gevoerd met

Afdeling /Team Informatiebeheer: Emile Wennink

Vervolgstappen en planning

Om scores te verbeteren moeten we de aanbevelingen zoveel mogelijk opvolgen. De aanbevelingen worden opgenomen in het actieplan Privacy en de belangrijkste aanbevelingen nemen we op in het Informatieveiligheidsplan. Hierin moeten we prioriteren. De acties uit het Informatieveiligheidsplan worden periodiek geëvalueerd.

Participatie

N.v.t.

Communicatie

N.v.t.