

FG Auditplan

Gemeente Dalfsen juni -december 2024

Door: mr. J
Functie: Functionaris Gegevensbescherming
Taakomvang: 18 dagen per jaar;
Periode: Juni 2024 – december 2024
Organisatie: Gemeente Dalfsen
Datum: 11 juni 2024
Versie: 1.1

Inhoud

1. Inleiding	3
2. Toelichting auditplan 2024.....	3
3. Gedetailleerd Auditplan	4
3.1 Audit Privacy managementsysteem (PMS)	4
3.2 Data Protection Impact Assessments (DPIA's)	5
3.3 Audit aanwezigheid en effectiviteit AVG beleid	6
3.4 Training- en Bewustwordingsaudits	7
3.5 Steekproefsgewijze audits	8
3.6 Derdenaudits	9
3.7 Beveiligingsaudits.....	10
3.8 Wpg audit	11
4. Planningsoverzicht audits juni -juli 2024 gemeente Dalfsen	12

1. Inleiding

Dit auditplan is opgesteld met als doel om de wettelijke toezichtstaak van de Functionaris voor Gegevensbescherming (FG) binnen Gemeente Dalfsen (hierna ook: de organisatie) effectief en aantoonbaar in te vullen.

Het plan biedt een gestructureerde aanpak voor het uitvoeren van diverse audits die gericht zijn op het waarborgen van naleving van de Algemene Verordening Gegevensbescherming (AVG).

Door middel van regelmatige en systematische audits wordt invulling gegeven aan de wettelijke vereisten, en wordt de organisatie gestimuleerd om continu te verbeteren. Dit auditplan dient als leidraad voor de FG en andere betrokken afdelingen om de integriteit, vertrouwelijkheid en beschikbaarheid van persoonsgegevens binnen de organisatie te waarborgen.

2. Toelichting auditplan 2024

In dit auditplan wordt aangegeven hoe de FG van de gemeente Dalfsen het komende jaar (medio 2024-medio 2025) invulling zal geven aan zijn controlerende taak door het uitvoeren van audits.

In deze periode zal het accent met name liggen op het controleren van het beleid en het privacymanagementsysteem binnen de gemeente. Zodra vastgesteld wordt dat er sprake is van een aantoonbaar deugdelijk privacymanagementsysteem zal de nadruk meer komen te liggen op gegevensverwerkingen binnen afdelingen en samenwerkingsverbanden.

Dit auditplan omvat zowel het toezicht op de AVG als op de Wpg binnen de gemeente Dalfsen.

3. Gedetailleerd Auditplan

In dit hoofdstuk wordt per auditonderdeel aangegeven op welke wijze de audit plaats zal vinden. Tevens wordt de omvang van de audit en de auditwijze toegelicht.

3.1 Audit Privacy managementsysteem (PMS)

Doelstelling:

Het beoordelen van de kwaliteit en de effectiviteit van het privacymanagementsysteem, de samenhang van beleid en systemen om de privacy binnen de organisatie te waarborgen.

Reikwijdte:

Beoordeling aanwezigheid en effectiviteit van beleid, procedures en praktijken.

Methode:

Vergelijk praktijken met AVG-vereisten, documenteer bevindingen en stel verbeteringen voor.

Frequentie:

halfjaarlijks

Verantwoordelijke(n):

- Actualisatie PMS: Privacy Officer
- toetsing: FG

Rapportage:

Auditverslag, onderdeel FG-jaarverslag en FG-halfjaarverslag

Aandachtspunt/bijzonderheden:

- het PMS zal in oktober 2024 worden beoordeeld.

3.2 Data Protection Impact Assessments (DPIA's)

Doelstelling:

- Identificeren en mitigeren van risico's voor de privacy van betrokkenen.
- Voldoen aan de wettelijke verplichting (art. 35 AVG)

Reikwijdte:

De beoordeling van (pre-)DPIA's waarin nieuwe verwerkingen, significante wijzigingen in bestaande verwerkingsactiviteiten waarbij omvangrijke, risicovolle of complexe persoonsgegevens worden verwerkt.

Methode:

- Beoordeling van pre-DPIA's om vast te stellen of men bij de afweging voor het uitvoeren van een DPIA de juiste keuzes heeft gemaakt;
- Beoordeling documentatie en advisering van de uitgevoerde DPIA conform de wettelijke FG-taken.

Frequentie:

Naar behoefte.

Tijdinschatting:

n.b.

Verantwoordelijke(n):

- Uitvoering DPIA's: procesverantwoordelijken met ondersteuning van de Privacy Officer.
- Beoordeling: FG

Rapportage:

Separaat FG-advies, onderdeel DPIA

Aandachtspunt/bijzonderheden:

De gemeente Dalfsen heeft nog geen DPIA's uitgevoerd.

Hierdoor loopt de gemeente risico. Een gemeente heeft tal van gevoelige verwerkingen waarbij een DPIA verplicht is.

Ik adviseer de gemeente Dalfsen om:

- Ten minste bij nieuwe of gewijzigde, DPIA-waardige verwerkingen, een DPIA uit te (laten) voeren;
- Waar mogelijk DPIA's uitvoeren op lopende verwerkingen waar een DPIA verplicht is.

Ik verwacht in de komende periode ten minste 4 DPIA's te ontvangen.

3.3 Audit aanwezigheid en effectiviteit AVG beleid

Doelstelling:

Het beoordelen van de kernprocessen die de organisatie in staat stellen om de AVG na te leven.

Reikwijdte:

In deze audit wordt getoetst:

1. Het privacybeleid van de organisatie;
2. Het beleid, de uitvoering en de registratie van de rechten van betrokkenen;
3. Het beleid, de uitvoering en de registratie van datalekken;
4. De aanwezigheid, kwaliteit en actualiteit van het Register van verwerkingsactiviteiten;
5. de informatievoorziening aan betrokkenen.

Methode:

1. Beoordeling van de actualiteit en juistheid van het privacybeleid;
2. Beoordeling logboeken van verzoeken, beoordeel reactietijden en naleving;
3. Beoordeling incidentlogboeken, meldings- en beoordelingsprocedure en responstijden;
4. Beoordeling van het register van verwerkingen;
5. beoordeling van de privacyverklaring.

Frequentie: Jaarlijks.

Tijdinschatting:

n.b.

Verantwoordelijke(n):

- Aanleveren documentatie: Privacy Officer
- Beoordeling: FG
- Rapportage: FG

Rapportage:

FG: auditverslag

Aandachtspunt/bijzonderheden:

Het vingerende beleid is geldig tot en met 2024. Het is zaak dat het privacybeleid dit jaar wordt vernieuwd.

3.4 Training- en Bewustwordingsaudits

Doelstelling:

Vaststellen op welke manier, en in hoeverre medewerkers op de hoogte zijn (gebracht) van de gegevensbeschermingsprincipes en het geldende beleid binnen de organisatie.

Reikwijdte:

- Training bij in diensttreding
- Uitingen (ver)nieuw(d) beleid
- Informatie aan inhuur/leveranciers

Methode:

- Beoordeling scholingsprogramma
- Beoordeling communicatie medewerkers
- interviews

Frequentie:

Jaarlijks.

Tijdinschatting:

n.b.

Verantwoordelijke(n):

- Aanleveren documentatie: Privacy Officer
- Beoordeling: FG
- Rapportage: FG

Rapportage:

FG: auditverslag

Aandachtspunt/bijzonderheden:

3.5 Steekproefsgewijze audits

Doelstelling:

Steekproefsgewijze beoordeling van interne procedures en werkwijzen op compliance met de AVG.

Reikwijdte:

Gegevensverwerking, beheer van rechten van betrokkenen, reactie op datalekken, gegevensbewaring.

Methode:

Interviews, documentbeoordelingen, observatie, testen.

Frequentie:

Halfjaarlijks

Tijdinschatting:

n.b.

Verantwoordelijke(n):

- Aanleveren documentatie: Privacy Officer
- Beoordeling: FG
- Rapportage: FG

Rapportage:

FG: auditverslag

Aandachtspunt/bijzonderheden:

3.6 Derdenaudits

Doelstelling:

Zorg voor naleving van gegevensbeschermingsvereisten door derden partijen, zoals belangrijke toeleveranciers, gemeenschappelijke regelingen en/of verwerkers.

Reikwijdte:

Verwerkersovereenkomsten, beveiligingsmaatregelen, nalevingsdocumentatie.

Methode:

Beoordeel contracten, voer leveranciersbeoordelingen uit, documenteer bevindingen.

Frequentie:

Jaarlijks.

Tijdinschatting:

n.b.

Verantwoordelijke:

- Aanleveren documentatie: Privacy Officer
- Beoordeling: FG
- Rapportage: FG

Rapportage:

Auditverslag.

Aandachtspunt/bijzonderheden:

-

3.7 Beveiligingsaudits

Doelstelling:

Waarborgen dat er passende technische en organisatorische maatregelen zijn genomen om de gegevens binnen de organisatie te beschermen.

Reikwijdte:

Beveiligingsmaatregelen, encryptie, toegangscontrole, incidentrespons.

Methode:

Beoordeling aanwezigheid van het informatiebeveiligingsbeleid, gesprek CISO over de effectiviteit van het informatiebeveiligingsbeleid.

Frequentie:

Jaarlijks.

Tijdinschatting:

n.b.

Verantwoordelijken:

CISO: aanleveren informatiebeveiligingsbeleid

FG: Beoordeling en verslaglegging

Rapportage:

Auditverslag (jaarverslag)

Aandachtspunt/bijzonderheden:

-

3.8 Wpg audit

Doelstelling:

Het doel van deze audit is om te beoordelen of de verwerking van politiegegevens binnen de gemeente Dalfsen voldoet aan de eisen van de Wet politiegegevens (Wpg) en de Algemene Verordening Gegevensbescherming (AVG).

Reikwijdte:

Wpg verwerkingen binnen de gemeente Dalfsen.

In 2024 zal het algemene Wpg beleid en het domein openbare ruimte worden geaudit, in 2025 ontwikkelingen in het Wpg beleid en de Wpg verwerkingen rond de Leerplicht.

Specifiek dient effectief toezicht gehouden te worden op:

- toezicht op doelbinding
- noodzakelijkheid & rechtmatigheid
- juistheid en volledigheid van gegevens
- gegevensbescherming door beveiliging en ontwerp
logging van verwerkingen zoals opgenomen in art 32a lid 1
- audits
- de formele aanwijzing van de FG

Methode:

Beoordeling van het beleid, interviews en steekproefsgewijze beoordeling van registraties in de BOA-systemen.

Frequentie:

Jaarlijks.

Verantwoordelijken:

PO: aanleveren beleid

BOA: interview, verstrekken steekproefsgewijs gewenste informatie

FG: Beoordeling en verslaglegging

Rapportage:

Auditverslag Wpg en FG-jaarverslag

Aandachtspunt/bijzonderheden:

-

4. Planningsoverzicht audits juli -december 2024 gemeente Dalfsen

	Audit Type	Frequentie	Maand/Kwartaal	Tijdsbegroting	Opmerkingen
3.1	Audit PMS	Halfjaarlijks	Oktober 2024	3 uur	
3.2	Data Protection Impact Assessments (DPIA's)	Naar behoefte	Doorlopend	Ntb	
3.3	Aanwezigheid en effectiviteit AVG beleid	Jaarlijks	November 2024	12 uur	
3.4	Training- en bewustwordingsaudits	Jaarlijks	December 2024	2 uur	
3.5	Steekproefsgewijze audits	Halfjaarlijks	Ntb	Ntb	
3.6	Derdenaudits	Jaarlijks	Augustus 2024	4 uur	
3.7	Beveiligingsaudits	Jaarlijks	December 2024	4 uur	
3.8	Wpg Audit	Jaarlijks	November 2024	6 uur	

Toelichting grondslagen

In dit document kunt u secties vinden die onleesbaar zijn gemaakt. Deze informatie is achterwege gelaten op basis van de Wet open overheid (Woo). De letter die hierbij is vermeld correspondeert met de bijbehorende grondslag in onderstaand overzicht.

J Art. 5.1 lid 2 sub e

Het belang van de openbaarmaking van deze informatie weegt niet op tegen het belang van de eerbiediging van de persoonlijke levenssfeer van betrokkenen