PRIVACYBELEID ANG
Versie 1.1
Privacy team

ANG, Montfoort, 1 februari 2019
Kenmerk: ANG117-0048HRM

DE ANG CONNECTIE
De verbindende factor tussen organisatie en informatie

Inhoudsopgave

1 Kernpunten

1.1 Voor wie?

Dit privacybeleidskader bevat managementafspraken tussen de directie en het management. De afspraken moeten worden nagekomen in alle gevallen dat persoonsgegevens worden gebruikt, opgeslagen of uitgewisseld.

1.2 Doel

Het doel van het privacybeleidskader is om te waarborgen dat ANG de privacywetgeving naleeft zodat er sprake is van behoorlijke en zorgvuldige verwerking van persoonsgegevens in overeenstemming met de wet.

1.3 Visie

ANG is een dienstverlenende en klantgerichte organisatie. Iedereen die werkzaam is binnen de organisatie is verantwoordelijk voor het verantwoord omgaan met persoonsgegevens en het waarborgen van de privacyrechten van personen. Nieuwe technologische ontwikkelingen, innovatieve voorzieningen, globalisering en een steeds meer digitale overheid stellen andere eisen aan de bescherming van gegevens en privacy. ANG is zich hier terdege van bewust en zorgt dat de privacy gewaarborgd blijft, onder andere door maatregelen op het gebied van informatiebeveiliging, dataminimalisatie, transparantie en gebruikerscontrole te treffen. De burger moet erop kunnen vertrouwen dat de verwerkers van deze data zorgvuldig en veilig met de persoonsgegevens omgaan.

1.4 Kernpunten

De directie:

- draagt verantwoordelijkheden op aan proceseigenaren;
- voorziet in faciliteren voor bewustwording bij de medewerkers;
- treft maatregelen voor privacy-incidentenmanagement inclusief datalekken;
- voorziet in een privacyteam dat ondersteunt in privacybeleidsvoering;
- handhaaft het privacybeleid. ANG stelt een Functionaris voor de Gegevensbescherming aan die toeziet op de borging van privacy binnen de organisatie.

1.5 Scope

Het privacybeleidskader van ANG is van toepassing op alle bedrijfsvoering voor zover hierbij gewerkt wordt met persoonsgegevens en ANG daar zeggenschap over heeft. Dit beleidskader is het algemene deel van het privacybeleid van ANG. Het is de kapstok voor het privacybeleid waaraan aanvullende regelingen zijn opgehangen, zoals procesplannen of regelingen voor het uitoefenen van rechten.

Het privacybeleid omvat zowel bedrijfsprocessen als onderliggende voorzieningen voor informatieverwerking. Het beleid is van toepassing op processen die ANG uitbesteedt, inkoopt of op een andere manier organiseert.

Het privacybeleid omvat de gehele ‘data life cycle’: van het genereren of verzamelen van gegevens, het dagelijks gebruik ervan en de gegevensopslag tot en met de archivering en vernietiging ervan. Het beleid is ook van toepassing op beveiligingsproblemen, namelijk meldplicht datalekken.

1.6 Raakvlakken en overlap met andere beleidsthema’s

Het privacybeleid heeft raakvlakken met andere beleidsthema’s of vertoont hiermee overlap, zoals integriteit, kwaliteit, informatiebeveiliging, personeel en organisatie en communicatie. Van belang hierbij is dat de doelen van de privacywetgeving worden behaald.

2 Privacymanagement

2.1 Privacymanagement

De directie van ANG is verantwoordelijk voor de naleving van privacywetgeving en handelt in dat kader proactief op basis van afweging van belangen en risico's bij de verwerking van persoonsgegevens zodat deze zorgvuldig, behoorlijk en in overeenstemming met de wet is.

2.2 Managementstructuur

De directie van ANG is verantwoordelijk voor het voorzien in passende privacywaarborgen bij de uitvoering van de werkzaamheden. Het privacyteam ondersteunt proceseigenaren en/of de directie daar waar nodig bij de uitvoering van het privacybeleid.

2.3 Toezicht

De Functionaris voor de Gegevensbescherming is de (interne) toezichthouder van ANG. De Functionaris voor de Gegevensbescherming ziet toe op de naleving van de privacywetgeving.

De directie informeert indien nodig interne en externe doelgroepen over de Functionaris voor de Gegevensbescherming.

De Functionaris voor de Gegevensbescherming:

- informeert en adviseert de directie, proceseigenaren en het privacyteam over de werking van het privacybeleid en nakoming van de wettelijke verplichtingen;
- houdt toezicht op de nakoming van het privacybeleid en de wettelijke verplichtingen;
- helpt privacyklachten tot een goed einde te brengen;
- adviseert bij privacyincidenten over ernst en omvang;
- beheert het privacybeleidskader;
- ziet toe op het beheer van het register van verwerkingen conform art. 30 AVG;
- controleert de naleving van afspraken van ANG en ketenpartners en eventueel ook in samenwerking met auditors;
- helpt het privacybeleid uit te dragen bij interne en externe doelgroepen;
- is het contactpunt voor landelijke privacytoezichthouders.

De Functionaris voor de Gegevensbescherming krijgt de nodige ruimte voor uitvoering van taken:

- De directie en de proceseigenaren zorgen ervoor dat de Functionaris voor de Gegevensbescherming naar behoren en tijdig wordt betrokken bij de verwerking van persoonsgegevens.
- De Functionaris voor de Gegevensbescherming wordt volledig geïnformeerd over aspecten van de bedrijfsvoering waarbij persoonsgegevens worden verwerkt of wanneer daartoe voornemens bestaan.
- De directie en de proceseigenaren ondersteunen de Functionaris voor de Gegevensbescherming door haar op haar verzoek toegang te geven tot verwerking van persoonsgegevens en hem de middelen te bieden voor professioneel onderzoek.
- De Functionaris voor de Gegevensbescherming kan vrij en onafhankelijk advies geven.

3 Privacybeleid

3.1 Algemeen

ANG is zich bewust van de maatschappelijke verantwoordelijkheid bij de verwerking van persoonsgegevens. Om deze reden voert ANG proactief privacybeleid op basis van dit beleidskader en bewaakt ANG de goede nakoming van wet- en regelgeving op het gebied van privacybescherming.

3.2 Noodzakelijke gegevensverwerking

Alle medewerkers verwerken persoonsgegevens uitsluitend voor de volgende doelen:

1. de uitoefening van publieke taken;
2. de nakoming van wettelijke plichten;
3. de vrijwaring van vitale belangen van betrokkene(n);
4. de totstandkoming of uitvoering van een overeenkomst waarbij een betrokkene partij is;
5. de behartiging van een gerechtvaardigd belang van ANG of een derde aan wie gegevens worden verstrekt tenzij het recht op de bescherming van de persoonlijke levenssfeer prevaleert.

3.3 Kapstokregeling

Dit privacybeleidskader heeft een algemeen karakter en een raamwerkfunctie (kapstokregeling). Het zoomt niet in op de spelregels die kunnen gelden voor specifieke activiteiten. Voor zover dit nodig is, wordt via procesplannen nadere invulling aan het privacybeleidskader gegeven.

3.4 Inachtneming bijzondere wettelijke voorschriften

Via dit privacybeleidskader geeft ANG uitvoering aan de Algemene Verordening Gegevensbescherming (AVG). Voor zover van toepassing, wordt er rekening gehouden met de bijzondere wettelijke voorschriften.

4 Gedragsnorm voor proceseigenaren

De directie verwacht van een proceseigena(a)r(en) een behoorlijke en zorgvuldige gegevensverwerking in overeenstemming met de relevante wet- en regelgevingen en een goede regievoering. Hierbij hoort ook bij toezicht op subproceseigenaren en de bewaking van de privacy in de ketensamenwerking.
Het privacybeleid zoals vastgesteld in procesplannen en uitwerkingen daarvan moet concreet zijn: voor iedereen dient duidelijk te zijn wie verantwoordelijk is voor wat. Goede regievoering veronderstelt dat de proceseigenaar zich bewust is van de privacy risico's die verband houden met zijn proces en voorziet in praktische oplossingen (proceswaarborgen) waarmee hij die risico's tegengaat.

4.1 Evenwichtige aanpak

Een proceseigenaar voert de regie over de verwerking van persoonsgegevens waar hij verantwoordelijk voor is. De proceseigenaar documenteert met behulp van zijn procesplan hoe hij op een praktische manier in passende organisatorische en technische privacybeschermende maatregelen voorzien om met name de volgende fouten te voorkomen:

1. Illegale gegevensverwerking: gebruik, opslag of uitwisseling van informatie is bij de wet verboden.
2. Disproportionele gegevensverwerking: gebruik, opslag of uitwisseling van informatie is (a) ontoereikend of juist overmatig, (b) het organisatiebelang bij de gegevensverwerking is klein terwijl personen door de gegevensverwerking substantieel benadeeld worden.
3. Onnauwkeurige gegevensverwerking: de gebruikte, opgeslagen of uitwisselde informatie is geen juiste weergave van de werkelijkheid.
4. Niet-inachtneming van bijzondere wettelijke voorschriften: bij gebruik, opslag of uitwisseling van informatie worden formele verplichtingen veronachtzaamd.
5. Onvoldoende afgewogen gegevensverwerking: bij keuzes over de opzet en werking van informatievoorzieningen wordt privacy meegewogen – om alle factoren in aanmerking genomen – te kunnen kiezen voor de meest privacyvriendelijke oplossing (subsidiariteit).
6. Irrelevante gegevensverwerking: de gebruikte, opgeslagen of uitwisselde informatie doet niet ter zake of is verouderd.
7. Onveilige informatieverwerking: de gebruikte, opgeslagen of uitwisselde informatie dreigt te gemakkelijk toegankelijk te zijn, gemanipuleerd te worden of niet beschikbaar te zijn.

4.2 Procesbeschrijving

De proceseigenaar legt de afspraken rond gegevensverwerkingen- en beveiliging (informatiebeleid), indien nodig, vast in een procesplan.
De proceseigenaar maakt een inventarisatie van de gegevensverwerking waar hij verantwoordelijk voor is. Hierbij kunnen identificerende gegevens, kwalificerende gegevens, procesgegevens, monitoringgegevens, conditionele gegevens en juridische gegevens worden onderscheiden.

4.3 Beheer procesplan

De proceseigenaar is verantwoordelijk voor het beheer van zijn procesplan. Als er sprake is van diverse subproceseigenaren, hoort de hoofdproceseigenaar in ieder geval goed geïnformeerd te zijn over de hoofdlijnen.

5 Privacyservices

5.1 Rechten

Betrokkenen hebben er recht op dat:

- ANG handelt volgens het onderhavige privacybeleidskader;
- dat ANG informatie verschaft over doelen van informatieverwerking en privacybeleidsvoering;
- dat zij bij niet-naleving van het privacybeleid of de wet ANG hierop mogen aanspreken.

5.2 Vragen en klachten

Bij vragen en klachten hebben betrokkenen het recht om zich te wenden tot het privacyteam van ANG. Dit kan telefonisch en/of per e-mail.

De vragen worden uiterlijk binnen 10 werkdagen afgehandeld.
De klachten worden zo snel mogelijk, maar uiterlijk binnen 4 weken afgehandeld.

6 Privacyprogramma

6.1 Bewustwording en training

De directie bevordert een privacybewuste organisatiecultuur via voorbeeldgedrag en door te overzien in de middelen voor bewustwording en, zo nodig, training van medewerkers.

6.2 Communicatie

De directie is transparant over de privacybeleidsvoering en voert op dit thema evenwichtig communicatiebeleid.

6.3 Informatievoorzieningen

De directie draagt zorg voor privacybestendige informatievoorzieningen en gegevensopslag. De proceseigenaren dragen hieraan bij.

6.4 Archiefbeleid, managementinformatie, gegevensvernietiging

De directie voorziet samen met proceseigenaren in met passende waarborgen omklede verdere verwerking van gegevens voor verenigbare doelen zoals het genereren van managementinformatie. Ook wordt voorzien in met passende waarborgen omklede oplossingen voor archivering en adequate oplossingen voor gegevensvernietiging.

6.5 Informatiebeveiliging

De directie ziet erop toe dat informatieveiligheid van ANG in lijn met de geldende norm wordt georganiseerd.

6.6 Regeling privacyincidenten

De directie voorziet in een procedure voor privacyincidenten die onder de verantwoordelijkheid van de Functionaris voor de Gegevensbescherming valt. De procedure privacyincidenten bevat in ieder geval een meldplicht voor gebeurtenissen die de beschikbaarheid, integriteit en vertrouwelijkheid van informatievoorzieningen en gegevensopslag aantasten.

6.7 Auditbeleid

Vragen, klachten en het incident management zijn in wezen steekproefsgewijze toetsing van de privacybeleidsvoering. Om niet voor verrassingen te worden geplaatst, is het de zaak dat proceseigenaren ook zelf periodiek laten controleren in hoeverre beleidsvoering en feitelijke situatie met elkaar overeenstemmen aan de hand van privacyaudits op de gehanteerde ijkpunten.

Quick scan: een beknopt toets onder de verantwoordelijkheid van de proceseigenaar.
Zelfevaluatie: een uitgebreidere toets onder de verantwoordelijkheid van de proceseigenaar.
Externe audit: een audit die de proceseigenaar organiseert in samenwerking met de FG en waarbij een professionele auditor wordt betrokken.

Op dit moment worden 24/7 quick scans uitgevoerd op alle ICT processen van ANG. Zowel inkomend als uitgaand verkeer wordt constant gemonitord op excessief dataverkeer dat er op zou kunnen wijzen dat er een beveiligingsinbreuk plaats vindt. Daarnaast worden frequent pentesten uitgevoerd op de computersystemen.