Overzicht van alle (ook eerder beantwoorde) OR-vragen over het privacybeleid

Jaarrapportage FG inzake het algemene AVG-volwassenheidsniveau

"Kun je nog een onderscheid maken tussen de verwerking van persoonsgegevens van medewerkers en die van derden?"

"Het volwassenheidsniveau is 2,3. De OR stelt voor om 3,0 als concreet streefdoel vast te leggen."

Het algemene AVG-volwassenheidsniveau van 2,3 is vastgesteld door de FG over het jaar 2024. Inmiddels is dat rapport enige tijd geleden verschenen en hebben we op onderdelen verdere voortgang geboekt. Op basis van de laatste interne inschattingen (onder meer vanuit de Privacy Officers en CIO-office) schatten we in dat we nu richting niveau 2,6 bewegen.

Met dit nieuwe beleid worden vervolgens gerichte en concrete stappen gezet richting niveau 3.0, dat breed wordt gezien als de ondergrens voor aantoonbare AVG-naleving. Na vaststelling van het beleid en uitvoering van het bijbehorende plan van aanpak, verwachten we dit niveau duurzaam te bereiken en te borgen.

Een herijking van het volwassenheidsniveau volgt na implementatie, en zal terug te vinden zijn in het jaarverslag van de FG over 2025. Een expliciete uitsplitsing tussen medewerkers- en derdengegevens is niet beschikbaar.

Plan van aanpak richting het algemene AVG-volwassenheidsniveau 3.0

"De OR verzoekt om een concreet plan van aanpak, inclusief tijdsplanning, voor de implementatie."

Samen met de FG werken we aan een plan van aanpak waarin de aanbevelingen uit het jaarrapport worden vertaald naar concrete acties. Doel is om uiterlijk eind 2026 het volwassenheidsniveau 3.0 te bereiken. De planning wordt afgestemd met het lijnmanagement en in het najaar met de OR gedeeld. Het is mogelijk dat het beoogde niveau al medio 2026 wordt bereikt. In dat geval zullen we de OR daarover uiteraard snel informeren.

Privacyverklaring

"Wij constateren dat er nog geen verwijzing is opgenomen naar (rechts)middelen wanneer een medewerker het niet eens is met een besluit van de provincie."

Dank voor deze terechte aanvulling. We nemen in de definitieve versie van de privacyverklaring een duidelijke alinea op over de mogelijkheid tot bezwaar. Daarbij verwijzen we naar de interne bezwaarprocedure en het recht om een klacht in te dienen bij de FG of de Autoriteit Persoonsgegevens. De technische omgeving is gereed; het formulier wordt na instemming met het beleid op het plein gepubliceerd, zodat medewerkers hun rechten eenvoudig kunnen uitoefenen.

Privacy-bewustzijn

"Wij verzoeken om een samenhangend pakket aan maatregelen voor bewustwording, zonder medewerkers te overspoelen."

We werken op dit moment aan een meer structurele bewustwordingsaanpak. Daarin combineren we e-learnings (de e-learnings zijn verplicht) met gerichte voorlichting aan CMT- en AMT-leden én aan afdelingen of teams. Dit wordt aangevuld met informele en vrijwillige initiatieven, zoals de laagdrempelige mini-cursussen en AI-kampvuurtjes die na de zomer van start gaan.

Een volledig samenhangend pakket is er nog niet, maar wordt in de loop van dit jaar verder ontwikkeld. Daarbij letten we nadrukkelijk op de balans tussen informatiedichtheid en toegankelijkheid, zodat medewerkers - uiteraard -niet overspoeld raken.

AVG-formulier inzake rechten van de betrokkenen (medewerkers)

Is het formulier voor AVG-rechten tijdig beschikbaar én gebruiksvriendelijk?

De technische omgeving is gereed; het formulier wordt na instemming met het beleid op het plein gepubliceerd, zodat medewerkers hun rechten eenvoudig kunnen uitoefenen. We toetsen de gebruiksvriendelijkheid vooraf met enkele collega's. Instructies en toelichting zijn opgenomen, zodat duidelijk is welke rechten medewerkers hebben en hoe zij die kunnen gebruiken.

Wet politie gegevens (WPG)

"Advies om ook de Wpg op te nemen in het privacybeleid voor een integraal overzicht."

De verwerking van politiegegevens door onze BOA's valt onder de Wpg en daarmee onder een ander juridisch kader dan de AVG. Het instemmingsrecht van de OR ziet niet op deze categorie gegevens. Deze verwerkingen zijn daarom niet opgenomen in dit privacybeleid. Tegelijk vinden wij het belangrijk dat ook BOA's als medewerkers goed geïnformeerd zijn over hun privacyrechten. We onderzoeken in welke vorm we hieraan invulling geven.

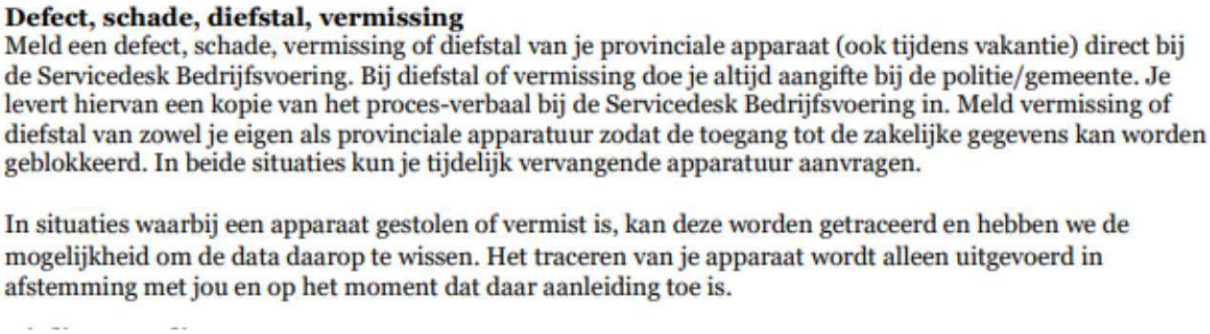
Personeelsvolgsysteem

"Maakt de provincie gebruik van een personeelvolgsysteem, in de zin dat bepaalde personen toegang hebben tot informatie over wat collega's invoeren in bijvoorbeeld DocBase?" "En heeft OGD toegang tot dergelijke data? Welke protocollen gelden hiervoor, waar zijn die te vinden?"

Er is geen sprake van structurele actieve volgsystemen. De provincie maakt geen gebruik van personeelsvolgsystemen in de zin van structurele monitoring van gedrag of prestaties van medewerkers.

Concreet betekent dit:

- Er is geen systeem dat structureel bijhoudt welke dossiers worden ingezien, welke toetsen of muisklikken worden gebruikt, of welke inhoud door medewerkers in systemen wordt geraadpleegd;
- Logging vindt uitsluitend plaats ten behoeve van beveiliging en auditing (zoals bij DocBase, waar wordt geregistreerd wie iets wijzigt, toevoegt of downloadt — maar niet wie iets bekijkt);
- Locatiegegevens van laptops en telefoons worden alleen gebruikt voor het verwijderen van de inhoud bij verlies of diefstal, waarbij er een melding op de betreffende laptop verschijnt dat de locatie is opgevraagd. Dit is tevens vermeld in de meest recente versie van de gebruikswijzer (die bijna iedereen heeft ondertekend):



Defect, schade, diefstal, vermissing
Meld een defect, schade, vermissing of diefstal van je provinciale apparaat (ook tijdens vakantie) direct bij de Servicedesk Bedrijfsvoering. Bij diefstal of vermissing doe je altijd aangifte bij de politie/gemeente. Je levert hiervan een kopie van het proces-verbaal bij de Servicedesk Bedrijfsvoering in. Meld vermissing of diefstal van zowel je eigen als provinciale apparatuur zodat de toegang tot de zakelijke gegevens kan worden geblokkeerd. In beide situaties kun je tijdelijk vervangende apparatuur aanvragen.

In situaties waarbij een apparaat gestolen of vermist is, kan deze worden getraceerd en hebben we de mogelijkheid om de data daarop te wissen. Het traceren van je apparaat wordt alleen uitgevoerd in afstemming met jou en op het moment dat daar aanleiding toe is.

- Voor wat betreft de infrastructuur (bijv. laptops en telefoons) is nu OGD, maar straks KPN de beheerder. Dit betekent dat de opvraag van gegevens (zoals hierboven genoemd) met medewerking van OGD (straks KPN) wordt gedaan. Dit gebeurt onder strikte voorwaarden zoals vastgelegd in de overeenkomst.

<u>Groot datalek personeelsdossiers – vervolgacties</u>
"Hoe voorkomen we dat dit opnieuw gebeurt? Worden er voorwaarden gesteld bij inkoopcontracten?"

Het datalek met personeelsdossiers bij een externe partij is destijds de aanleiding geweest voor mijn aanstelling als privacy officer. Sindsdien is er veel veranderd. De afdeling P&O weet inmiddels goed wat er vanuit de AVG van haar verwacht wordt om dit soort incidenten in de toekomst te voorkomen. Zo hebben we ervoor gekozen om de migratie van personeelsdossiers hier op kantoor te laten uitvoeren (dit is al gebeurd)–> onder onze eigen regie.

Ook binnen de inkoopprocessen zijn concrete stappen gezet. Inkoop verwijst nu standaard naar de AVG in alle procedures, ongeacht het type opdracht. Privacy is daarmee structureel onderdeel geworden van het inkoopproces. We hebben wekelijks overleg met inkoop om ervoor te zorgen dat de AVG-afspraken goed worden vastgelegd.

Dat betekent dat privacyvraagstukken sneller in beeld komen en eerder opgepakt kunnen worden. Bij samenwerking met externe partijen hanteren we standaard

verwerkersovereenkomsten én aanvullende eisen op het gebied van informatiebeveiliging, zoals ISO 27001-certificering.

Voor projecten met verhoogde privacyrisico's voeren we een DPIA uit, waarbij ook expliciet wordt getoetst of de betrokken verwerker voldoet aan de vereisten van de AVG. Zo zorgen we ervoor dat uitbesteding niet alleen efficiënt en doelmatig gebeurt, maar ook veilig en controleerbaar. Alles met het oog op het voorkomen van herhaling van het datalek uit het verleden.

Gedragscodes

Werkt de provincie conform een gedragscode?

Kun je aangeven wat je hiermee bedoelt? Daar waar het gaat om de verwerking van persoonsgegevens onder de AVG, geldt het privacybeleid straks in ieder geval als het centrale kader voor al onze privacyactiviteiten. Dit beleid bevat normerende uitgangspunten en concrete verplichtingen die in de praktijk de functie van een gedragscode vervullen. Zo beschrijft het beleid op een toegankelijke manier de kernprincipes van gegevensverwerking, zoals:

- **Doelbinding, dataminimalisatie en juistheid** (zie p. 8, §2.2.2 en §2.2.4),
- **Integriteit, vertrouwelijkheid en beveiliging** (p. 9–10, §2.2.5 en p. 13, §2.3.6),
- **Transparantie naar betrokkenen en rechtmatigheid** (p. 9–10, §2.2.6 en §2.2.7).

Daarnaast zijn er in de bijlagen concrete werkprocessen en gedragslijnen opgenomen voor onder meer:

- **Gebruik van e-mail, het delen van persoonsgegevens, en opslag in systemen zoals SharePoint** (zie proces "Verwerkingen en overeenkomsten met derden", p. 18 e.v.) + bestaand beleid dat te vinden is op het plein onder bijv. veilig mailen, sharepoint: Support: Handleidingen Privacy en AVG, docbase: DocBase info Regels voor het registreren in DocBase.
- **Omgang met datalekken** (proces "Datalekken", p. 25 e.v.),
- **Rechten van betrokkenen** zoals inzage-, wijzigings- of verwijderverzoeken (p. 30 e.v.). Dat ging voorheen per e-mail/identificatie op locatie > zie privacyverklaring voor derden die al heel lang op onze website staat (niet verwarren met die van de medewerkers uiteraard): Privacyverklaring . Nu kunnen derden een verzoek ook indienen via digid-omgeving op onze website. Medewerkers straks ook via het plein (hier zijn wij momenteel mee bezig). Het plein zal straks ook worden gebruikt om het privacybeleid voor de medewerkers bekend te maken.

ISO-27001 certificering

Is de provincie ISO-27001 gecertificeerd voor informatiebeveiliging?

Ja, de provincie is hiervoor gecertificeerd.

Is Trustboand-systeem, dat door de privacy-organisatie wordt gebruikt, ISO-27001 gecertificeerd?

De provincie werkt met Trustbound voor DPIA's, het verwerkingsregister en datalekregistratie. Dit ondersteunt de aantoonbaarheid van privacymaatregelen. Is ook ISO-27001 gecertificeerd.

Met bovenstaande toelichting vertrouwen wij erop alle vragen van de OR te hebben beantwoord. Mocht er behoefte zijn aan nadere afstemming of toelichting op onderdelen, dan horen we dat graag.

Met vriendelijke groet,