Provincie Antwerpen

Dienstnota van de provinciegriffier

Nummer:	**DAB– 21 - 2022**
Onderwerp:	**Gedragscode voor databeheerders - Hoe omgaan met informatie**
Inhoudelijk contactpersoon:	Katty Scholdis (DPO)
Samenvatting:	Deze dienstnota legt de regels vast die in acht dienen genomen te worden door de databeheerders die werkzaam zijn binnen het provinciebestuur Antwerpen. De dienstnota is van toepassing op iedereen die meer rechten heeft dan de gewone gebruikersrechten. Dit geldt dus voor onder andere: ontwikkelaars, systeembeheerders, informatiebeheerders, applicatiebeheerders, netwerkbeheerders, consultants, onderaannemers,… (niet limitatieve lijst)
Bronnen:	
Van toepassing op:	Medewerkers van de binnen- en buitendiensten en volgende APB's en EVAP's: APB PVM / APB POA (niet-gesubsidieerd personeel) / APB PRZ / APB PRDS / APB PIH / APB PSES / APB PDA / APB GKC / APB KMPC / APB HH APB CVST / APB TPA / APB WAR / APB HC EVAP AK / EVAP PSRN / EVAP PRLB / EVAP SKL / EVAP PV

Deze dienstnota treedt in werking op **20/06/2022**

Deze dienstnota vervangt dienstnota DAB–21/2016

Inhoudstafel

Gedragscode voor databeheerders - Hoe omgaan met informatie

Van toepassing voor ontwikkelaars, systeembeheerders, informatie-beheerders, applicatiebeheerders, netwerkbeheerders, consultants, onderaannemers,… (niet exhaustieve lijst).

1. Inleiding en draagwijdte

Het doel van deze gedragscode is de regels vast te leggen die in acht moeten worden genomen door de databeheerders die werkzaam zijn binnen de groep Provincie Antwerpen.

Deze gedragscode past binnen het informatieveiligheidsbeleid dat door de provinciegriffier en het MT is goedgekeurd en is een uitwerking van één van de beheersmaatregels inzake informatieveiligheid.

2. Toepassingsgebied

Niemand zal er vandaag de dag nog aan twijfelen dat ICT een cruciale rol speelt in het economisch leven. Het behoorlijk functioneren van netwerken, systemen en toepassingen is van groot belang voor talloze overheden, bedrijven en particulieren die in grote mate "afhankelijk" zijn van hun ICT infrastructuur en, bij uitbreiding, ook van hun databeheerders.

Alvorens de rollen en de verantwoordelijkheden van de databeheerders verder toe te lichten is het nuttig om de opdrachten van de Data Protection Officer (DPO) toe te lichten. De DPO is immers ertoe gehouden de wetten met betrekking tot de bescherming van het privéleven te doen naleven. Hij heeft tevens een adviserende, stimulerende, documenterende, controlerende en bevorderende opdracht inzake naleving van de veiligheidsregels die door een wettelijke of reglementaire bepaling of krachtens dergelijke bepaling zijn opgelegd. Hij moet er ook voor zorgen dat de personen die binnen de organisatie werken een veiligheidsbevorderende houding aannemen. In dat opzicht is hij/zij vanzelfsprekend een bevoorrechte partner van de databeheerders.

De databeheerder is eenieder die toegangsrechten heeft die dat van het functioneel gebruik van de gegevens overschrijden. ***Het gaat met name om ontwikkelaars, systeembeheerders, informatiebeheerders, applicatiebeheerders, netwerkbeheerders, consultants en onderaannemers (niet exhaustieve lijst).***

Deze code heeft niet de ambitie om de precieze taak van de databeheerder te omschrijven of om een technische handleiding te zijn voor databeheerders. Dat is immers al gebeurd in andere documenten (oa. arbeidsreglement, diverse nota's binnen DICT, jaarafspraken met betrokken medewerkers,…). De code kan al evenmin een concrete oplossing bieden voor elk ethisch of beleidsprobleem waarmee een databeheerder kan geconfronteerd worden in de uitvoering van zijn functie.

Wel wil de code alle databeheerders bewust maken van het belang hun bevoegdheden op een ethisch verantwoorde manier uit te oefenen: de integriteit van een databeheerder maakt deel uit van zijn professionaliteit. De databeheerder kan dus de code gebruiken als richtsnoer bij het maken van beleids- en andere keuzes. Bovendien moet de databeheerder de code zien als een voortdurende uitnodiging om zijn professioneel handelen ethisch te toetsen en waar nodig aan te passen.

Voor de overige werknemers van de onderneming is het nuttig te weten dat de uitoefening van de bevoegdheden van de databeheerder ingebed is in regels. Voor de werkgever is het nuttig om te preciseren hoe de databeheerder gebruik moet maken van zijn bevoegdheden in het belang van de onderneming.

3. Vereisten

3.1 De integriteit, beschikbaarheid en de vertrouwelijkheid van de informatie

3.1.1. De databeheerder staat in voor het behoorlijk functioneren van één of meerdere systemen (hardware, software, netwerkapparatuur, enz.) van de ICT infrastructuur. De databeheerder mag enkel die handelingen stellen die nodig zijn om de integriteit en de beschikbaarheid van het systeem te verzekeren of te verbeteren.

> *Toelichting: De databeheerder onthoudt er zich met andere woorden van professionele handelingen te verrichten voor enig ander doel dan het verzekeren van de goede werking van het computersysteem in het belang van de onderneming.*

3.1.2. Hij waakt er tevens over dat deze handelingen niet leiden tot het verlies van data of een inbreuk op de authenticiteit en de integriteit van de gegevens tot gevolg heeft.

3.1.3 Aangezien bepaalde handelingen van gebruikers schade kunnen berokkenen aan de integriteit, authenticiteit of de beschikbaarheid van het computersysteem of –netwerk, of de gegevens, moet de databeheerder in het kader van zijn verantwoordelijkheden toezien op de naleving van het beleid van toepassing in de organisatie. Dit houdt in dat hij naar gelang de ernst van vastgestelde feiten die schade aan integriteit, authenticiteit of beschikbaarheid tot gevolg hebben, hiërarchisch meerderen hierover informeert.

Indien hij vaststelt dat bepaalde van deze acties niet onder het toepassingsgebied van bestaande policy 's vallen, brengt hij de DPO hiervan op de hoogte. De DPO zal dan de nodige maatregelen treffen in het belang van het provinciebestuur en/of de verzelfstandigde entiteit.

3.1.4 Databeheerders waken erover dat toegang tot het systeem en haar data slechts wordt verleend volgens de gangbare procedures. Om zo er voor te zorgen dat toegang voorbehouden blijft aan diegenen voor wie dergelijke toegang vereist is uit hoofde van hun functie.

Indien hij vaststelt dat toegangsprocedures niet werden nageleefd of dat bepaalde toegangsvragen niet vallen onder bestaande procedures, brengt hij de DPO hiervan op de hoogte. De DPO zal dan de nodige maatregelen treffen in het belang van de het provinciebestuur en/of de verzelfstandigde entiteit.

3.2 Informatiebescherming

Naleving van de privacywetgeving en bescherming van de persoonsgegevens

3.2.1 De databeheerders hebben toegang persoonsgegevens waarop de bepalingen inzake bescherming van het privéleven en van de persoonsgegevens van toepassing zijn.

> *Toelichting: onder "persoonsgegeven" wordt verstaan iedere informatie betreffende een geïdentificeerde of identificeerbare natuurlijke persoon, hierna genaamd "betrokken persoon". Als identificeerbare persoon wordt beschouwd een persoon die rechtstreeks of onrechtstreeks geïdentificeerd kan worden, met name aan de hand van een identificatienummer of van één of meerdere specifieke elementen die kenmerkend zijn voor zijn of haar fysieke, fysiologische, psychische, economische, culturele of sociale identiteit.*

3.2.2 De databeheerder is zich bewust van het feit dat de persoonsgegevens moeten worden beschermd. Hij ziet er dus nauwgezet op toe deze regels na te leven, met bijzondere aandacht voor de regels inzake verwerking van persoonsgegevens waaruit de raciale of etnische afkomst, de politieke opvattingen, de godsdienstige of levensbeschouwelijke overtuiging of het lidmaatschap van een vakvereniging blijkt, alsook de verwerking van gegevens met betrekking tot gezondheid of seksuele oriëntatie.

3.2.3 De databeheerder neemt passende technische en organisatorische maatregelen met betrekking tot de beveiliging en bescherming van persoonsgegevens, tegen toevallige of ongeoorloofde vernietiging, tegen toevallig verlies evenals tegen de wijziging van of de toegang tot, en iedere andere niet toegelaten verwerking van persoonsgegevens.

3.2.4 De databeheerder waakt erover dat ook derden de bepalingen met betrekking tot de bescherming van het privéleven naleven.

> *Toelichting: bijvoorbeeld bij onderhoud of herstelling van het computersysteem door derden. Ook zij moeten op de hoogte zijn van de relevante verplichtingen inzake de bescherming van de persoonsgegevens*

Controle van de online communicatie en toegang tot de bestanden

3.2.5. De databeheerder mag de elektronische online communicatie en de toegangen tot de bestanden controleren binnen het kader van zijn bevoegdheden en mits de naleving van de wettelijke en reglementaire bepalingen.

> *Toelichting: Deze reglementaire bepalingen zijn vastgelegd in dienstnota - Informatieveiligheid (DAB-24-2021).Wat de controle op het gebruik van internet en e-mail betreft, is er een specifieke procedure gemaakt, die terug te vinden is in het arbeidsreglement.*

Vertrouwelijke gegevens

3.2.6 De databeheerder gaat ervan uit dat alle informatie van de organisatie vertrouwelijk is en als dusdanig behandeld moet worden. Hij is *-net als elke andere medewerker van het provinciebestuur en/of verzelfstandigde entiteit-* verplicht om vertrouwelijke informatie geheim te houden voor iedereen die niet bevoegd is om er kennis van te nemen.

Toelichting: het gaat bijvoorbeeld niet alleen om persoonsgegevens, maar ook over beroepsgeheimen, know-how of andere gevoelige gegevens.

3.2.7 De databeheerder verbindt zich ertoe vertrouwelijke gegevens niet te gebruiken of te circuleren binnen de onderneming behoudens voor zover strikt noodzakelijk voor de uitoefening van zijn functie.

Toelichting: In het kader van zijn functie heeft de databeheerder vaak toegang tot allerlei vertrouwelijke gegevens. Het is van belang dat de databeheerder deze vertrouwelijkheid niet enkel extern respecteert, maar tevens intern binnen de onderneming zelf.

3.3 Informatie- en documentatieplicht

3.3.1 De databeheerder licht de gebruikers duidelijk in over het toegelaten gebruik van het informatiesysteem.

3.3.2. De databeheerder licht naar aanleiding van een interventie zijn handelingen toe opdat de betrokken gebruiker voldoende geïnformeerd zou zijn over de gevolgen hiervan op het gebruik van het systeem. Deze informatie moet tijdig en op een begrijpelijke manier worden meegedeeld.

Toelichting: het gaat om de interventies van de databeheerder, bijvoorbeeld in het kader van de aanpassing van een systeem.

3.3.3. De databeheerder waakt erover dat er steeds een geactualiseerde documentatie voorhanden is waarin het systeem (bijv. ontwikkeling, hard- en software, infrastructuur) op zodanige wijze wordt beschreven dat elke betrokken persoon zich een totaalbeeld zou kunnen vormen van dit systeem. De bedoeling ervan is een continu beheer van het systeem te garanderen.

Toelichting: het gaat om het geval waarin de databeheerder om de een of andere reden zijn functie niet meer kan uitoefenen. Een andere databeheerder moet het systeem dan verder doeltreffend kunnen beheren. Hiervoor is een goede inventaris van de infrastructuur vereist.

4. Reglementering

De moedwillige niet-naleving van deze gedragscode kan aanleiding geven tot een sanctie overeenkomstig de binnen de organisatie van kracht zijnde procedures.

5. Toepassingsgebied

De dienstnota is volledig van toepassing op de APB's en EVAP's.

6. Onderhoud, opvolging en herziening

Het onderhoud, de opvolging en de herziening van deze gedragscode zijn de verantwoordelijkheid van de DPO van provinciebestuur Antwerpen.

Maarten Ronny Puls
De Provinciegriffier

23/06/2022