Borging privacy op P4 data

ODA zomersessie 7 juli 2017

Datum: 7-7-2017
Erik Linschoten: Senior Projectadviseur Slimme Meters Liander / Voorzitter Beleidscommissie Privacy en Security Slimme meters Netbeheer Nederland

As-Is Proces toestemming

Wetgeving is basis > E- en G wet:

Een netbeheerder verleent een derde uitsluitend toegang tot meetgegevens betreffende afnemers als bedoeld in artikel 95a, eerste lid, voorzover die derde de desbetreffende meetgegevens op basis van artikel 8, onderdeel a, van de Wet bescherming persoonsgegevens mag verwerken.

- Afnemers zijn kleinverbruikers (in technische zin)
- WBP art. 8a = Ondubbelzinnige toestemming van de klant

Ook art 79 E-wet (geheimhoudingsverplichting NB's) is van toepassing

As-Is proces hoe het nu ingericht is m.b.t ODA's:

- De ondubbelzinnige toestemming van de klant (klantmandaat) wordt door ODA's per EAN aan de verschillende netbeheerders aangeleverd
- Dit is feitelijk een verklaring van de ODA dat er toestemming van de klant verkregen is
- De netbeheerder levert op basis van deze verklaring de data via P4
- De verantwoording van de ODA of de klant ook echt die toestemming heeft verleend, vindt achteraf plaats d.m.v. een jaarlijks op te leveren assurance-verklaring

Geen ideaal proces

- De toezichthouders ACM (toezichthouder E- en G-wet) en Autoriteit Persoonsgegevens (AP; toezichthouder WBP) melden zich ook nadrukkelijker, mede gedreven door incidenten; bijv. identiteitsfraude via ODA of datalek bij een LV. En doen ook uitspraken:
  - NB's en marktpartijen vormen een keten
  - NB's moeten voorafgaand aan dataverstrekking, per opvraging, aanwezigheid van een mandaat controleren
  - Meer 'Privacy Minded' denken in de sector. Er moet voortaan echt meer vanuit de WBP worden gekeken naar vraagstukken.

- Achteraf controleren van toestemming lijkt dus niet toekomstbestendig
- Denk ook aan problematiek bij verhuizingen

- Algemene verordening gegevensverwerking (AVG) – nog wat strenger, in aantoonbaarheid van voldoen aan privacy wetgeving. Voor alle partijen in de keten
- AVG Art 5 lid 2 > De verwerkingsverantwoordelijke is verantwoordelijk voor de naleving van lid 1 en kan deze aantonen („verantwoordingsplicht").

AVG art 5 lid 1

Algemene Verordening Gegevensbescherming (AVG) art 5 lid 1

1. Persoonsgegevens :

a) („rechtmatigheid, behoorlijkheid en transparantie”) richting betrokkene

b) („doelbinding”) voor het verwerken van gegevens

c) („minimale gegevensverwerking”); beperkt tot wat noodzakelijk is voor de doeleinden waarvoor zij worden verwerkt

d) juist zijn en zo nodig worden geactualiseerd; alle redelijke maatregelen moeten worden genomen om de persoonsgegevens die, gelet op de doeleinden waarvoor zij worden verwerkt, onjuist zijn, onverwijld te wissen of te rectificeren („juistheid”);

e) betrokkenen niet langer te identificeren dan voor de doeleinden waarvoor de persoonsgegevens worden verwerkt noodzakelijk is („opslagbeperking”);

f) passende technische of organisatorische maatregelen op een dusdanige manier dat een passende beveiliging van persoonsgevens gewaarborgd is, en dat zij onder meer beschermd zijn tegen ongeoorloofde of onrechtmatige verwerking en tegen onopzettelijk verlies, vernietiging of beschadiging („integriteit en vertrouwelijkheid”).

Algemene Verordening Gegevensbescherming (AVG)

- De AVG betekent dat organisaties nog bewuster moeten omgaan met de bescherming van persoonsgegevens.
- De AVG betekent ook dat organisaties nog meer rekening moeten houden met de rechten van betrokkenen. Belangrijke rechten zijn:
    - Het recht om vergeten te worden
    - Het recht op export van data wanneer wordt overgegaan op een andere leverancier
    - Het recht op informatie over een hack (meldplicht datalekken)
    - Privacyverklaringen moeten in duidelijke taal worden opgesteld
- Melding van verwerking bij AP wordt vervangen door een verantwoordelijkheid om alle verwerkingen te documenteren.
- ‘privacy by design’ en ‘privacy by default’: In het kader van de gegevensbescherming is nieuw dat dit moet worden geëxpliciteerd.
- **Speciale aandacht voor toestemming:** Organisaties moeten kunnen bewijzen dat zij geldige toestemming hebben gekregen. En moet het voor mensen net zo makkelijk zijn om hun toestemming in te trekken als om die te geven.

Visie NBNL op data/privacy

Netbeheerder als betrouwbare en onafhankelijke datamanager

- Data niet voor andere doeleinden gebruiken dan waarvoor ze zijn verkregen
- Zonder toestemming of wettelijke basis delen de NB's persoonsgegevens niet met derde partijen.
- Een NB toont proactief aan hoe hij invulling geeft aan de privacywetgeving.
- Transparantie

De klant staat centraal en is in de lead

- NB ondersteunt de klant door gegevens (zoals zijn energiegebruik) aan marktpartijen ter beschikking te stellen. De klant moet hiervoor zelf toestemming geven en kan zijn verleende toestemming beheren in een toestemmingenregister.

Bescherming van de privacy als leidend principe

- NB handelt volgens het principe van *privacy by design*.

Verbeteren van een gelijk speelveld en markttoegang

- Gegevens ter beschikking stellen op non-discriminatoire wijze

Verhogen van doelmatigheid voor het beheer en het ontwikkelen van energiesystemen

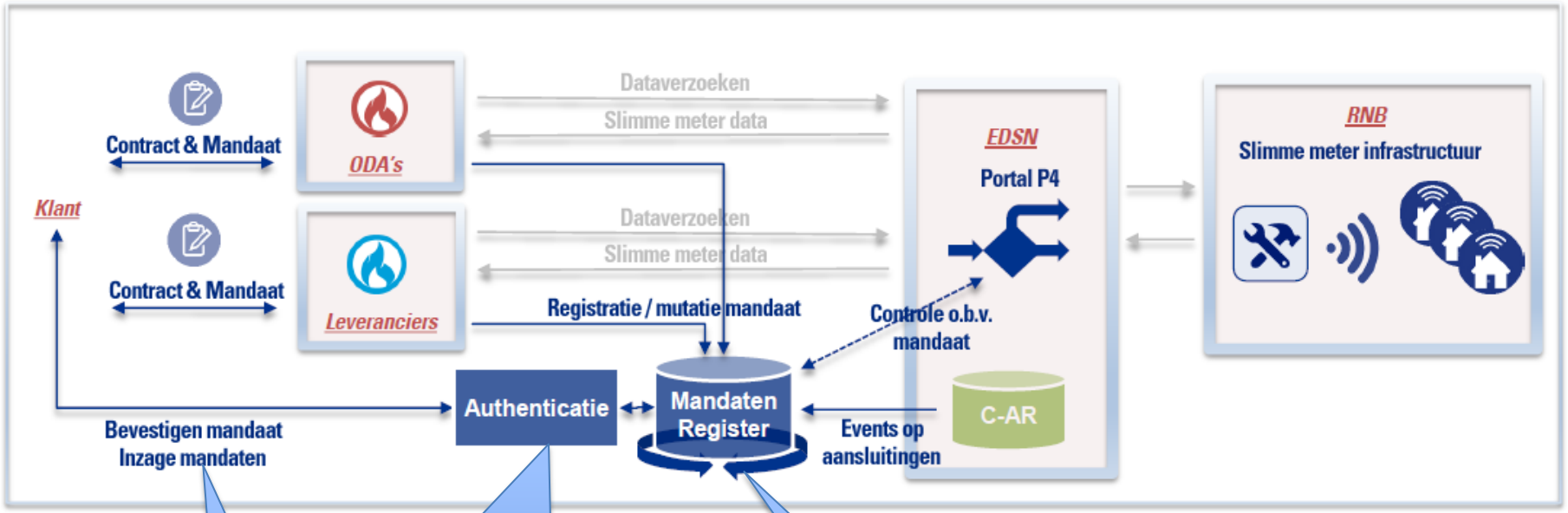
- Gebruik van data tbv energietransitie mits onder de juiste voorwaarden

Toestemmingenregister

- Verschillende mogelijkheden

- Maar ook al bekende problemen/issues o.a:
  - Definitie van de klant die toestemming moet geven:
    - Contractant: degene met wie ODA een ovk heeft
    - Afnemer: degene met wie de NB een ovk (ATO) heeft.
    - Betrokkene: terminologie WBP – degene ‘die de deur open doet’
  - Klantidentificatie/authenticatie: Op basis van welk mechanisme?
    - Notificatie-brieven/mails
    - Publieke authenticatie middelen zoals Idensys/Idin
    - …
  - + Adrescontrole: waar klant woont, is van belang omdat gegevens op adres/EAN worden verstrekt
  - Zakelijke klanten (met een KVB aansluiting)

Toestemmingenregister



Ook intrekken mandaat hoort hierbij

Verschillende mogelijkheden. Idensys/IDIN ?

Centraal gepositioneerd

Discussie