

An aerial photograph of an industrial park. In the center, a large white wind turbine stands prominently. To its right, a long industrial building features a roof covered in solar panels. The park is situated near a body of water on the left. The sky is blue with scattered white clouds. The word 'EIGEN' is printed in large, white, stylized letters in the upper right corner of the image.

**EIGEN**

# Privacy en security Energy Hubs

**Auteur: Pelle van den Heuvel**

**Datum: 21 augustus 2025**

---

## Inleiding

Dit memo geeft een overzicht van de algemene en specifieke regelgeving die van toepassing is op verschillende assets binnen een Energy Hub, daarbij zal met name worden ingegaan op de benodigde vergunningen. Hierbij zal onderscheid worden gemaakt in regels en vergunningplichten die voor alle assets gelden enerzijds, en regels en vergunningplichten die specifiek voor een bepaalde asset gelden anderzijds.

## Mededingingsrecht

Voor de relevante privacy en security regelgeving is ten eerste van belang of er energie wordt uitgewisseld in de Energy Hub. Wanneer er sprake is van afspraken binnen een Energy Hub tussen partijen die (normaliter) concurrenten van elkaar zijn. Het mededingingsrecht is cruciaal in situaties waarin concurrenten samenwerken, zoals binnen een Energy Hub. Deze regels beschermen de markt tegen oneerlijke concurrentie en waarborgen de belangen van consumenten.

Concurrenten mogen onder het mededingingsrecht geen concurrentiegevoelige informatie met elkaar delen, zoals prijsstrategieën, klantgegevens of toekomstplannen. Dergelijke informatie-uitwisseling kan leiden tot marktvervalsing of kartelvorming, tenzij er een gegronde reden of wettelijke uitzondering geldt.

Binnen een Energy Hub bestaat het risico dat deelnemende partijen andere marktspelers buitensluiten, wat kan leiden tot een machtspositie en concurrentiebeperking. Dergelijk gedrag valt onder het verbod op misbruik van economische machtspositie.

Afspreken dat alleen bepaalde partijen mogen deelnemen aan een Energy Hub, kan de toegang tot de markt ernstig belemmeren. Tenzij deze afspraken aantoonbaar bijdragen aan efficiëntie en voordelen voor consumenten opleveren, zijn ze in strijd met het mededingingsrecht.

## Privacy en de AVG

In Energy Hubs wordt veel data verzameld en gedeeld, bijvoorbeeld energieverbruiksgegevens van huishoudens of kleine ondernemers. Dit zijn persoonsgegevens en vallen onder de Algemene Verordening Gegevensbescherming (AVG). Voor Energy Hubs betekent dit dat gegevensverwerking alleen mag plaatsvinden op basis van een wettelijke grondslag of expliciete toestemming van de betrokkenen. Daarnaast moeten Energy Hubs het principe van dataminimalisatie naleven, bewaartermijnen

---

beperken en ervoor zorgen dat data alleen voor het afgesproken doel wordt gebruikt.

In de praktijk leidt dit tot vragen over de rol van netbeheerders en andere partijen bij het aansturen van flexibiliteit. Om compliant te blijven, moeten Energy Hubs duidelijke afspraken maken in verwerkingsovereenkomsten en waar mogelijk werken met geaggregeerde data, zodat individuele privacy wordt beschermd terwijl toch inzicht voor congestiemanagement wordt geleverd.

## Cyber security

Voor het goed functioneren van een Energy Hub is uitwisseling van informatie tussen systemen essentieel. Deze gegevensuitwisseling vindt op drie momenten plaats:

- **Vooraf:** Informatie over gepland verbruik, verwachte opwekking, netwerkgrenzen en prijsverwachtingen;
- **Real-time:** Meetdata van verbruik, productie, stuursignalen en assetstatus;
- **Achteraf:** Facturatie en prestatie-registratie.

Om deze gegevens te beschermen, moeten er proportionele cybersecuritymaatregelen getroffen worden. Bescherming is nodig tegen risico's als:

- **Verlies van vertrouwelijkheid:** Onbevoegde verspreiding van gevoelige gegevens;
- **Verlies van integriteit:** Ongeautoriseerde wijziging of vernietiging van data;
- **Verlies van beschikbaarheid:** Tijdelijke of langdurige onderbreking van toegang tot informatie.

De impact van dergelijke incidenten kan variëren van risico's voor fysieke veiligheid en reputatieschade tot financiële verliezen, milieuschade, wettelijke overtredingen of uitval van energievoorziening.

## NIS2

De herziene NIS2-richtlijn, die sinds januari 2023 van kracht is en uiterlijk oktober 2024 volledig geïmplementeerd moet zijn, beoogt een hoog cybersecurityniveau in de hele EU. De herziene NIS2-richtlijn verplicht essentiële sectoren, waaronder energie, tot een hoog niveau van cyberbeveiliging. Energy Hubs vallen onder deze regels omdat zij deel uitmaken van kritieke infrastructuur. Concreet houdt dit in

---

dat Energy Hubs incidenten binnen 24 uur moeten melden, structureel risicobeheer moeten aantonen en dat bestuurders persoonlijk aansprakelijk kunnen worden gesteld bij nalatigheid.

Voor Energy Hubs betekent dit dat gezamenlijke incidentresponsprocessen en crisisprotocollen moeten worden ingericht. Omdat een hub meerdere organisaties omvat, is coördinatie tussen partners noodzakelijk: een incident bij één partij kan de hele hub raken. Daarnaast moeten Energy Hubs aantonen dat hun digitale infrastructuur structureel beveiligd is en dat continu wordt gewerkt aan veerkracht.

Belangrijkste kenmerken van NIS2:

- **Snelle incidentmelding:** Binnen 24 uur na ontdekking moet melding worden gedaan bij bevoegde instanties;
- **Aanscherping van toezicht:** Niet naleven kan leiden tot sancties zoals boetes en persoonlijke aansprakelijkheid voor bestuurders;
- **Uitbreiding van sectoren:** NIS2 geldt voor meer sectoren dan zijn voorganger;
- **Samenwerking binnen EU:** Lidstaten moeten informatie delen en cybersecurity coördineren;
- **Versterking van veerkracht:** Organisaties worden verplicht om hun digitale infrastructuur structureel te beveiligen.

De richtlijn legt de lat hoger en zorgt dat alle lidstaten een gelijk niveau van bescherming nastreven.

## ISO 27001

ISO 27001 biedt een internationaal erkend raamwerk voor informatiebeveiliging en kan dienen als gezamenlijke standaard voor Energy Hubs. Het implementeren van ISO 27001 helpt om vertrouwelijkheid, integriteit en beschikbaarheid van informatie systematisch te waarborgen. Concrete maatregelen zoals encryptie, toegangsbeheer, monitoring en verplichte risicobeoordelingen maken Energy Hubs minder kwetsbaar voor cyberaanvallen en datalekken.

Door gebruik te maken van ISO 27001 kunnen Energy Hubs vertrouwen opbouwen tussen partners, voldoen aan AVG- en NIS2-eisen en makkelijker samenwerken met overheden, klanten en financiers. Bovendien biedt de norm ondersteuning bij noodplannen en herstelprocedures, zodat operationele processen ook tijdens incidenten doorgang vinden.

---

## Tot slot

In dit memo is een vereenvoudigde weergave gegeven van de regelgeving die binnen het kader van privacy en security van toepassing is op Energy Hubs. Voor gedetailleerdere informatie kunt u contact opnemen met het EIGEN platform.