Het Normo
duidelijke afspraken ■ veilige energiedata

Extern incidentenprotocol

Versie: 1.0
Datum: 20 juli 2026

Inhoudsopgave

1. Meldplichten van Het Normo

1.1 Juridisch kader

Het Normo als gegevensuitwisselingsentiteit in het kader van de Energiewet is verplicht incidenten te melden bij relevante toezichthouders en instanties, op basis van wettelijke en contractuele verplichtingen, zoals:

Wettelijke basis	Wat melden	Aan wie	Termijn
Artikel 4.22 Energiewet	Een inbreuk op de beveiliging van gegevens met aanzienlijke gevolgen voor: a. de toegang tot en uitwisseling van gegevens; of b. de aangeslotene wiens gegevens het betreft.	Rijksdienst Digitale Infrastructuur ("**RDI**")	Onverwijld
Artikel 33 Algemene Verordening Gegevensbescherming	Een inbreuk in verband met persoonsgegevens. (meer specifiek: een inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte persoonsgegevens)	Autoriteit Persoonsgegevens ("**AP**")	Zonder onredelijke vertraging en, indien mogelijk, uiterlijk 72 uur nadat Het Normo er kennis van heeft genomen
Artikel 34 Algemene Verordening Gegevensbescherming	Een inbreuk in verband met persoonsgegevens die waarschijnlijk een hoog risico inhoudt voor de rechten en vrijheden van natuurlijke personen	Betrokkenen	Onverwijld
Cyberbeveiligingswet (NIS2)[1]	Significante incidenten (meer specifiek: een incident is een gebeurtenis die de beschikbaarheid, authenticiteit, integriteit of vertrouwelijkheid van opgeslagen, verzonden of verwerkte gegevens of van de diensten die worden aangeboden door of toegankelijk zijn via netwerk-	Computer Security Incident Response Team ("**CSIRT**") in de vorm van het Nationaal Cyber Security Centrum ("**NCSC**") en de bevoegde toezichthouder. Incidenten kunnen worden gemeld via	Zo snel mogelijk, maar in ieder geval binnen 24 uur na waarneming van het incident (vroegtijdige waarschuwing)

[1] De GUE is op moment van vaststelling van dit protocol nog niet aangewezen als kritieke entiteit onder de Wet weerbaarheid kritieke entiteiten.

	en informatiesystemen, in gevaar brengt. Een incident is significant als het een ernstige verstoring van de diensten of financiële verliezen voor de organisatie veroorzaakt of kan veroorzaken óf andere entiteiten heeft getroffen of kan treffen door aanzienlijke materiële of immateriële schade te veroorzaken. In welke specifieke gevallen hiervan sprake is, wordt nog met sectorspecifieke drempelwaarden nader uitgewerkt in ministeriële regelingen).	het NCSC-portaal (mijn.ncsc.nl). Het NCSC stuurt de melding vervolgens door naar de sectorale CSIRT en de relevante toezichthouder (waarschijnlijk het RDI).	
Wet beveiliging netwerk- en informatiesystemen (NIS1)	De meldplicht onder deze wet is niet van toepassing op Het Normo. Mocht Het Normo vrijwillig willen voldoen, dan geldt de meldplicht voor ernstige digitale veiligheidsincidenten die de samenleving kunnen ontwrichten. Het is ook mogelijk een vrijwillige melding te doen.	NCSC	Zo snel mogelijk en in ieder geval binnen 24 uur
Regels Registerbeheerders	Incidenten gerelateerd aan (de beveiliging van) Gegevens en/of Registers (zoals gedefinieerd in de Regels Registerbeheerders van Het Normo).	De Registerbeheerder (zoals gedefinieerd in de Regels Registerbeheerders van Het Normo)	Onverwijld
Regels Systeemprocespartij	Incidenten gerelateerd aan (de beveiliging van) systemen en verbindingen voor de Gegevensuitwisseling Systeemprocessen.	De Systeemprocespartij (als gedefinieerd in de Regels Systeemprocespartij van Het Normo)	Zo spoedig mogelijk
Regels Dataverzoekendepartij	Incidenten gerelateerd aan de Faciliteit en/of Dataproduct (als gedefinieerd in de Regels Dataverzoekendepartij van Het Normo)	De Dataverzoekendepartij (als gedefinieerd in de Regels Dataverzoekendepartij van Het Normo).	Onverwijld

1.2 Meldplicht aan Het Normo

Naast de eigen meldplichten van Het Normo, is een aantal partijen verplicht Het Normo te informeren in geval een incident zich voordoet die is gerelateerd aan de faciliteit die Het Normo aanbiedt:

Basis	Wat melden	Termijn
Regels Registerbeheerder	Incidenten gerelateerd aan (de beveiliging van) Gegevens en/of Registers	Onverwijld
Regels Dataverzoekendepartij	Incidenten gerelateerd aan de Faciliteit en/of een Dataproduct Daarbij dient in ieder geval die informatie te worden verstrekt aan Het Normo die de Dataverzoekendepartij ook moet delen met de desbetreffende autoriteiten.	Onverwijld
Regels Systeemprocespartij	De Systeemprocespartij is verplicht om incidenten gerelateerd aan (de beveiliging van) Gegevensuitwisseling Systeemprocessen onverwijld te melden bij Het Normo conform het incidentenprotocol zoals dat door Het Normo op zijn website is gepubliceerd.	Zo spoedig mogelijk

Bij het uitvoeren van deze meldplichten, dienen partijen zich volgens de van toepassing zijnde Regels te houden aan onderstaand incidentenprotocol.

2. Incidentenprotocol

Dit incidentenprotocol ("**Incidentenprotocol**") beschrijft hoe incidenten moeten worden gemeld aan Het Normo.

2.1 Wat is een incident?

Een incident als bedoeld in dit Incidentenprotocol is:

- Iedere inbreuk op de beveiliging of beschikbaarheid van de faciliteit van Het Normo;
- Iedere inbreuk op de beschikbaarheid, integriteit of vertrouwelijkheid van de gegevens die via Het Normo (kunnen) worden opgevraagd of verstrekt, waaronder begrepen de registers van registerbeheerders;
- Iedere verstoring van de energievoorziening of kritieke dienstverlening als het de gegevensuitwisseling via Het Normo raakt of kan raken;
- Een datalek waarbij persoonsgegevens die Het Normo verwerkt zijn betrokken; en
- Ieder ander (beveiligings-)incident dat leidt, of kan leiden, tot aanzienlijke gevolgen voor de toegang tot en uitwisseling van gegevens via Het Normo, of voor de aangeslotene wiens gegevens het betreft.

(hierna gedefinieerd als: "**Incident**").

Enkele voorbeelden van Incidenten zijn onder meer (maar niet beperkt tot):

- Cyberaanvallen, malware of ransomware die leidt tot één of meer van de hierboven omschreven situaties;
- Ongeautoriseerde toegang tot de systemen of de faciliteit van Het Normo;
- Verstoringen van netwerk- en informatiesystemen die van invloed zijn op de dienstverlening van Het Normo;
- DDoS-aanvallen op de faciliteit;
- Verstoringen in de energievoorziening;
- Storingen aan het energienetwerk;
- Incidenten die de betrouwbaarheid of veiligheid van de energievoorziening bedreigen;
- (Vermoedelijk) verlies, diefstal of ongeoorloofde toegang tot persoonsgegevens die Het Normo verwerkt;
- Onbedoelde verstrekking van persoonsgegevens die Het Normo verwerkt aan onbevoegden; en
- Onbedoelde vernietiging of wijziging van persoonsgegevens die Het Normo verwerkt.

2.2 Uw meldplicht

Iedere persoon die een Incident constateert, of een vermoeden heeft dat een Incident heeft plaatsgevonden of zal plaatsvinden, dient dit **onverwijld** te melden aan Het Normo. Dit betekent zo snel mogelijk na ontdekking of bij het ontstaan van het vermoeden van een Incident.

Let op: Incidenten dienen bij Het Normo gemeld te worden ongeacht de vermeende ernst van het Incident.

2.3 Hoe moet u melden?

Incidenten kunt u melden als aangegeven op de website van Het Normo.

Urgente incidenten die directe aandacht van Het Normo vereisen moeten gemeld worden via het spoednummer. Dit is bijvoorbeeld het geval indien er een vermoeden is van een succesvolle cyberaanval op de faciliteit, een grootschalig datalek of een storing die grote invloed heeft of kan hebben op partijen.

- **Telefoonnummer voor urgente meldingen: 033-3037322.**

Let op: uw melding aan Het Normo ontslaat u niet van andere (wettelijke) meldplichten. Onderzoek daarom altijd of u het Incident ook bij andere partijen moet melden, zoals de bevoegde toezichthouder(s), het Nationaal Cyber Security Centrum, relevante contractspartijen of de politie.

2.4 Welke informatie heeft Het Normo nodig?

Via de website van Het Normo kunt u uw melding van een Incident indienen. Hiertoe is Het Normo de daarin gevraagde informatie van u en uw organisatie benodigd.

Gegevens die u vanwege de (privacy)wetgeving of andere juridische geheimhoudingsverplichtingen niet mag verstrekken, mag u in de initiële melding achterwege laten.

Waar nodig voor de beoordeling, registratie, afhandeling of melding van het Incident, kan Het Normo aanvullende informatie bij u opvragen. U dient Het Normo te allen tijde gevraagde medewerking te verlenen.

2.5 Wat doet Het Normo na uw melding?

Het Normo onderzoekt de melding en neemt waar nodig passende maatregelen om de gevolgen van Incidenten zo veel mogelijk te beperken.

✓ Onmiddellijke actie

1. Ontvangstbevestiging: U ontvangt zo spoedig mogelijk een bevestiging van ontvangst.
2. Eerste beoordeling: Wij beoordelen de ernst en urgentie van het Incident.
3. Registratie: Het incident wordt binnen Het Normo geregistreerd en bewaard zo lang als nodig voor de afwikkeling van het Incident.

✓ Vervolgstappen

1. Onderzoek: Wij onderzoeken de aard, omvang en oorzaak van het Incident.
2. Het treffen van mitigerende maatregelen: Indien de melding ziet op of raakt aan de faciliteit of andere systemen van Het Normo, dan treft Het Normo passende maatregelen om de gevolgen van het Incident zo veel mogelijk te beperken.
3. Meldingen aan autoriteiten: Het Normo meldt het Incident waar nodig bij relevante toezichthouders, instanties en andere partijen (zoals betrokken Registerbeheerders, Dataverzoekendepartijen of Systeemprocespartijen).
4. Informatie aan de Rijksdienst Digitale Infrastructuur (RDI): Het Normo verstrekt aan de RDI namens de Minister op zijn verzoek de informatie die nodig is om een gemeld Incident te beoordelen. Indien openbaarmaking in het algemeen belang is, kan de RDI een Incident openbaar maken of Het Normo verplichten tot openbaarmaking.
5. Statusupdates: Waar mogelijk wordt u op de hoogte gehouden over het Incident en de afhandeling ervan.
6. Evaluatie: Waar passend evalueert Het Normo de oorzaak van het Incident om de kans op herhaling te verkleinen.

2.6 Uw verantwoordelijkheden

Om het Incident en de gevolgen ervan zoveel mogelijk te beperken, dient u zich te houden aan het volgende:

- **Bereikbaarheid:** U zorgt ervoor dat u goed bereikbaar bent op de door u doorgegeven contactgegevens. Waar nodig geeft u wijzigingen in de contactgegevens tijdig aan Het Normo door.
- **Bewaren van informatie**: Bewaar alle relevante informatie, bewijsstukken en logs met betrekking tot het Incident en verstrek kopieën daarvan op verzoek aan Het Normo.
- **Medewerking**: Verleen alle redelijke medewerking aan Het Normo en bevoegde toezichthouders bij het onderzoek naar en de afwikkeling van het Incident.

- **Maatregelen**: Implementeer waar nodig passende beveiligingsmaatregelen om vergelijkbare incidenten in de toekomst te voorkomen, beperken en/of de aanpak ervan te verbeteren.

Vertrouwelijkheid

Het Normo behandelt alle Incidentmeldingen strikt vertrouwelijk. Informatie wordt alleen gedeeld met andere partijen voor zover dit wettelijk verplicht of noodzakelijk is voor de afhandeling van het Incident of voor de rapportageverplichtingen van Het Normo onder de Energiewet.

2.7 Meldplicht van Het Normo aan partijen

Op grond van de Regels van Het Normo heeft Het Normo in gevallen de verplichting partijen op de hoogte te stellen van Incidenten. Het Normo maakt hiervoor gebruik van het e-mailadres dat een partij bij registratie bij Het Normo heeft opgegeven. Deze partij dient ervoor te zorgen dat het opgegeven e-mailadres juist is en dient eventuele wijzigingen tijdig aan Het Normo door te geven.

2.8 Vragen?

Voor vragen over dit Incidentenprotocol kunt u contact opnemen via de website van Het Normo.