Nr	ISO hiërarchie	Omschrijving	Description
1.0.0	Beheersdoelstelling	Toegangsbeveiliging binnen de slimme-meterinfrastructuur is ingericht.	Access security in the advanced metering infrastructure is implemented.
1.1.0	Beheersmaatregel	Systeemassets in de slimme-meterinfrastructuur dienen enkel geauthenticeerde en geautoriseerde berichten te accepteren.	System Assets in the advanced metering infrastructure should only accept authenticated and authorised messages.
1.1.1	Implementatierichtlijn	Hierbij geldt dat sleutels voor de meter aan de volgende eisen dienen te voldoen: - minimaal 10 karakters lang, - samengesteld uit de set met alfanumerieke tekens (kleine letters, hoofdletters en cijfers), en - willekeurig en niet-herleidbaar ('pseudo random') gegenereerd.	Hereby applies that for keys for the meter, the following requirements should be met: - At least 10 characters long, - Composed of the set of alphanumeric characters (lowercase, uppercase and numbers), and - Random and non-traceable ('pseudo random') generated.
1.1.2	Implementatierichtlijn	Het verkrijgen van ongeoorloofde toegang tot één meter mag niet leiden tot het verkrijgen van toegang tot meerdere meters.	Getting unauthorized access to a single meter, should not result in getting access to several meters.
1.1.3	Implementatierichtlijn	Hierbij geldt dat wachtwoorden en beveiligingssleutels altijd per meter uniek dient te zijn vanaf het moment van installatie van de meter. Dit betreft ook expliciet APN-logingegevens voor GPRS en LTE en Domein inloggegevens voor CDMA.	Hereby applies that passwords and security keys, always per meter, should be unique from the time of installation of the meter. This includes explicitly APN login information for GPRS and LTE and Domain login information for CDMA.
1.1.4	Implementatierichtlijn	Netbeheerder dient alle af-fabriek wachtwoorden en sleutels voor de meter direct bij de eerste communicatie met het centraal systeem, te vervangen.	Grid operators should replace all factory-included passwords and keys for the meter, directly at the first communication with the central system.
1.1.5	Implementatierichtlijn	Netbeheerders hebben een sleutel- en wachtwoordbeleid vastgelegd en geïmplementeerd voor alle wachtwoorden in de slimme-meterinfrastructuur. In dit beleid stellen netbeheerders een termijn vast waarbinnen wachtwoorden en sleutels worden gewijzigd.	Grid operators have a key and password policy defined and implemented, for all passwords in the advanced metering infrastructure. By means of this policy the grid operators shall set a deadline, by which passwords and keys are changed.
1.2.0	Beheersmaatregel	Wachtwoorden en beveiligingssleutels dienen binnen een redelijke termijn vervangen te worden na compromittering. De redelijke termijn wordt enerzijds bepaald door het minimaliseren van de te behalen baten voor een potentiele kwaadwillenden, anderzijds bepaald door de technische mogelijkheden van de netbeheerder.	Passwords and security keys should be replaced within the period, determined by the policy, after being breached. The determined period is on the one hand defined by the potential benefits for a hacker, and on the other hand defined by the technical capabilities of a grid operator.
1.2.1	Implementatierichtlijn	De netbeheerder moet in staat zijn de gecompromiteerde wachtwoorden en beveiligingssleutels te vervangen.	The grid operator must be capable to replace compromised passwords and security keys.
1.2.2	Implementatierichtlijn	De redelijke termijn van het vervangen van wachtwoorden en beveiligingssleutels bij compromiteren is maximaal twee weken, er van uitgaande dat het gewin van een potentiele hacker bij voorbaat is ingeperkt.	The reasonable term for the replacement of compromised passwords en security keys is 2 weeks max, based on the assumption that a potential hackers gain has been limited in advance.
1.3.0	Beheersmaatregel	Meters die operationeel in gebruik zijn dienen altijd verzegeld te zijn.	Meters that are operational, should always be sealed.
1.4.0	Beheersmaatregel	De netbeheerder dient autorisatiebeheer voor systeemassets in de slimme-meterinfrastructuur te hebben vastgelegd en geïmplementeerd waarbij de netbeheerder controle heeft over de toegang tot de slimme-meterinfrastructuur.	Within the grid operator an authorisation management for system assets in the advanced metering infrastructure should be established and implemented, whereby the grid operator has control on the access to the advanced metering infrastructure.

1.4.1	Implementatierichtlijn	Autorisatiebeheerprocedures dienen te worden verwerkt in het kwaliteitsbeheersysteem van de netbeheerder. Ten minste eenmaal per jaar wordt gecontroleerd of de rechten van personen met toegang tot de slimme meterinfrastructuur nog kloppen met hun functie.	Authorisation management procedures should be included in the quality management system of the grid operator. At least once a year, the grid operator checks whether the rights of persons with access to the advanced metering infrastructure are consistent with their function (duty in the organisation).
1.5.0	Beheersmaatregel	Medewerkers van de netbeheerder dienen enkel toegang te hebben tot die functionaliteit en informatie in de slimme-meterinfrastructuur die nodig is voor de werkzaamheden die zij verrichten uit hoofde van hun functie.	Employees of the grid operators should have only access to that functionality and that information in the advanced metering infrastructure, which is needed for the work they carry out according to their function (duty in the organisation).
1.5.1	Implementatierichtlijn	Netbeheerders leggen autorisaties vast in een autorisatiematrix die up-to-date wordt gehouden. Toegang wordt alleen binnen een vastgelegd autorisatieproces toegekend, gewijzigd en ontnomen. Dit geldt ook voor alle betrokken externen.	Grid operators should record authorisations in an authorisation matrix, which is up-to-date. Access is granted, modified and deprived only within a defined authorisation process. This also applies to all external staff of the grid operator.
1.6.0	Beheersmaatregel	Het uitvoeren van kritieke systeemfuncties in de slimme-meterinfrastructuur dient alleen onder verhoogd toezicht en op basis van functiescheiding plaats te vinden.	The operations of critical system functions in the advanced metering infrastructure, should only take place under increased supervision, and on the basis of separation of duties.
1.6.1	Implementatierichtlijn	De volgende activiteiten worden als kritieke systeemfuncties in de slimme-meterinfrastructuur beschouwd: - het updaten van software. - het beheer van sleutels en wachtwoorden. - commissioning van meters.	The following activities are regarded as critical system functions: - Updating software. - Management of keys and passwords. - Commissioning of meters.
1.6.2	Implementatierichtlijn	Waar technisch mogelijk, moet logging van de uitgevoerde activiteiten plaatsvinden. Deze logging bevat tenminste metadata.	Logging the execution of critical system functions is mandatory, provided that it is technically possible. These loggings will contain meta data at the least.
1.6.3	Implementatierichtlijn	Logging vindt plaats van handelingen met kritieke systeemfuncties van systeemassets in de slimme-meterinfrastructuur. Logging dient te herleiden te zijn naar unieke natuurlijke personen.	There is logging of actions with the critical system functions of system assets in the advanced metering infrastructure. Logging must be traceable to unique individual persons.
1.7.0	Beheersmaatregel	Een E-meter dient enkel aan te sturen en te configureren te zijn via de P3-poort.	An E-meter can only be operated or configured through its P3 port.
1.8.0	Beheersmaatregel	Een G-meter dient enkel aan te sturen en te configureren te zijn via de P2-poort.	A G-meter can only be configured or operated through its P2 port.
2.0.0	Beheersdoelstelling	De netbeheerder beheerst het incidentmanagement.	The grid operator controls the incident management.
2.1.0	Beheersmaatregel	Netbeheerders en Netbeheer Nederland hebben onderling procedures vastgelegd en geïmplementeerd over hoe wordt omgegaan met privacy- en informatiebeveiligingsincidenten die schade aan de hele sector zouden kunnen veroorzaken.	Grid operators and the branch organisation Netbeheer Nederland have established and implemented procedures on how to deal with privacy and information security incidents that could damage the entire sector.

2.1.1	Implementatierichtlijn	Netbeheerders beschikken over een systeem waarin zowel privacy- als informatiebeveiligingsincidenten betreffende de slimme-meterinfrastructuur worden geregistreerd. Dit systeem voorziet een sectorbreed incidentregister tijdig en juist van informatie over incidenten. Netbeheerder beoordeelt de incidenten en meldt het incident indien noodzakelijk in het sectorbrede incidentenregister. Netbeheerders registreren incidenten conform eigen incidentmanagement en handelen deze af. Netbeheer Nederland beoordeelt de sectorbreed gemelde incidenten op sectorbrede impact en handelt deze, wanneer van toepassing, sectorbreed af. Hierbij geldt dat zowel het register bij de netbeheerder als het sectorbrede incidentregister enkel toegankelijk moet zijn voor speciaal daarvoor bevoegde medewerkers van de netbeheerders.	For the advanced metering infrastructure individual grid operators will register both privacy incidents and information security incidents in an incident registry. This system will feed a sector-wide incident registry with accurate and up-to-date information concerning these incidents. The individual grid operator will analyse each incident and determine if such incident should be forwarded to the sector-wide registry. Netbeheer Nederland will analyze forwarded incidents in terms of sector impact and will take appropriate sector-wide actions. Access to individual and sector-wide registries must be limited to specifically assigned employees.
2.2.0	Beheersmaatregel	Netbeheerder voorkomt en detecteert ongeautoriseerde toegang tot, en wijzigingen aan de slimme-meterinfrastructuur. Indien deze zaken niet door een netbeheerder zelf worden uitgevoerd dient dit contractueel geborgd te zijn bij leveranciers.	The grid operator prevents and detects unauthorized access to, and modifications in the advanced metering infrastructure. If these things are not performed by a grid operator itself, it should then contractually secured at the relevant vendors / suppliers.
2.2.1	Implementatierichtlijn	Bij ongeautoriseerde toegang tot de slimme-meterinfrastructuur geldt dat: - functionaliteit op meters en niet in of uit te schakelen is zonder dat de netbeheerder dit opmerkt. - fysieke en logische koppelingen binnen de slimme-meterinfrastructuur op afstand verifieerbaar zijn door de netbeheerder - bij storing of ontkoppeling van een P2-verbinding door de meter een waarschuwing gegenereerd wordt voor het centraal systeem. - meters detecteren fysieke aanvallen en genereren een waarschuwing voor het centraal systeem.	The following applies in case of unauthorized access to the advanced metering grid: - enabling or disabling functionality on meters cannot occur without detection by the grid operator - physical and logical interfaces (connections) can always be verified by the grid operator - malfunctioning or decoupling of any P2 device will trigger the meter to generate a warning for the central system -meters detect physical tampering and will generate a warning for the central system.
2.3.0	Beheersmaatregel	Netbeheerders hebben procedures en instructies die beschrijven hoe medewerkers omgaan met privacy- en informatiebeveiligingsincidenten vastgelegd en geïmplementeerd en dragen deze actief uit naar hun medewerkers.	Grid operators have recorded and implemented procedures and instructions that describe how employees deal with privacy and information security incidents. Grid operators actively reach out to their employees about this topic.
2.3.1	Implementatierichtlijn	Netbeheerders hebben sectorbreed procedures gedefinieerd en geïmplementeerd waarin enerzijds is vastgelegd hoe informatie uit incidenten wordt verwerkt in beleid om deze structureel te voorkomen en anderzijds is vastgelegd hoe in geval van crises snel op incidenten geacteerd en gereageerd kan worden.	Grid operators have defined and implemented sector-wide incident related procedures that describe how lessons learned are translated into prevention policies. They will also have sector-wide procedures in place that enable quick response to incidents in a time of crisis.

2.4.0	Beheersmaatregel	Netbeheerder dient te borgen dat processen gedefinieerd en geïmplementeerd zijn om alle in de slimme-meterinfrastructuur gegenereerde events te beoordelen en om passende acties te ondernemen wanneer dit kan leiden tot een incident.	The grid operator must guarantee that processes are defined and implemented for the generated events by the meter or data router, to assess it and take appropriate steps where this could lead to an incident.
2.5.0	Beheersmaatregel	Netbeheerder dient te borgen dat processen gedefinieerd en geimplementeerd zijn om gevolgen van incidenten te beperken.	The Grid Operator will ensure that processes are defined and implemented for the purpose of mitigation of the consequences of incidents .
2.6.0	Beheersmaatregel	De netbeheerder heeft processen vastgelegd en geïmplementeerd om verdachte en niet-correcte communicatie van zowel meters (via P3) als van derden (via P4) te registreren, beoordelen en om passende actie te ondernemen.	The grid operator has established and implemented processes to deal with suspicious and incorrect communication of both meters (through P3-port) as of third parties (through P4-port). The processes will cover registering, assessing and taking appropriate action.
2.7.0	Beheersmaatregel	De netbeheerder heeft technische oplossingen geimplementeerd om verdachte en niet-correcte communicatie (anomaliedetectie) van zowel apparaten (via P3) als van derden (via P4) te signaleren en loggen.	Suspicious and incorrect communication of both devices (via P3-port) as third parties (through P4-port) is identified and logged ('anomaly detection') by the grid operator.
2.8.0	Beheersmaatregel	Netbeheerders hebben procedures en instructies geïmplementeerd die beschrijven hoe medewerkers omgaan met een inbreuk in verband met persoonsgegevens (datalek) aan de toezichthoudende autoriteit (AP) (AVG art. 33) en mededeling van een inbreuk in verband met persoonsgegevens aan de betrokkene (AVG art. 34).	DSO's have implemented procedures and instructions describing how employees deal with a personal data breach to the supervisory authority (AP) (AVG Article 33) and notification of a personal data breach to the data subject (AVG art. 34).
3.0.0	Beheersdoelstelling	De netbeheerder handhaaft een acceptabel beveiligingsniveau voor nieuwe en bestaande systeemassets.	The grid operator maintains an acceptable level of security for new and existing system assets.
3.1.0	Beheersmaatregel	Netbeheerders dienen de beveiligingseisen voor systeemassets in acceptatietests te toetsen om vast te stellen dat beveiligingsfunctionaliteit van geleverde systeemassets juist en volledig is geïmplementeerd. Bij een negatieve uitkomst van de acceptatietests worden tekortkomingen in de beveiligingsfunctionaliteit verholpen vóór ingebruikname van systeemassets.	To determine if the security functionality of the delivered system assets is properly and fully implemented, the grid operators will test the security requirements for system assets against the security requirements in the form of acceptance tests. In case of a negative outcome during the acceptance tests the shortcomings in the security functionality are solved, before the system assets become operational.
3.2.0	Beheersmaatregel	Niet-noodzakelijke functionaliteit is uitgeschakeld of is door de netbeheerder op afstand uit te schakelen ('hardening'). Hiervoor geldt dat de netbeheerder een overzicht van de beschikbare functionaliteit van systeemassets heeft.	Unnecessary functionality is turned off, or the grid operator has the possibility to remotely disable ('hardening') this functionality. The grid operator maintains an overview of the available functionality of system assets.
3.3.0	Beheersmaatregel	Netbeheerder dient te borgen dat bij het ontwerp van meters geanalyseerd wordt welke wijzigingen in de beveiligingsfunctionaliteit mogelijk zijn in verband met de levensduur van deze functionaliteit ("toekomstvastheid").	In the design stage of meters, the grid operators will analyse to what extent the security functionality is future proof.
3.3.1	Implementatierichtlijn	In het functioneel ontwerp moet een analyse zijn opgenomen die een afweging maakt tussen kosten, capaciteit en risico.	The functional design must encompass an analysis of the trade-off between cost, capacity and risk.

3.3.2	Implementatierichtlijn	Bij het opstellen van functionele eisen bij meters en data routers moet rekening worden gehouden met voldoende capaciteit (bijvoorbeeld geheugen, processor, opslag etc.) om toekomstige wijzigingen, tengevolge van een veranderende dreigingshorizon aan te kunnen.	The functional requirements for meters and data routers must consider sufficient capacity (memory, processor, data storage) to meet future demands caused by a changing threat horizon.
4.0.0	Beheersdoelstelling	De netbeheerder neemt maatregelen om te zorgen dat kleinverbruikers standen niet manipuleren.	The grid operator shall take measures to ensure that private consumers will not manipulate measurement data.
4.1.0	Beheersmaatregel	In schriftelijke afspraken met de kleinverbruiker is vastgelegd dat de metergegevens, de communicatiefunctie en de meetfunctie niet gemanipuleerd of geblokkeerd mogen worden.	In written agreements with the private consumer is stated that the measurement data, the communication function and the measurement function should not be manipulated or blocked.
4.1.1	Implementatierichtlijn	Afspraken met kleinverbruikers kunnen netbeheerders afdwingen door middel van de aansluit- en transport overeenkomst (ATO). Communicatie vindt plaats overeenkomstig Informatiecode.	Grid operators can enforce consumer contracts using the ATO agreement (connection & transportation agreement). Communication will comply to the Information Code.
5.0.0	Beheersdoelstelling	De installatie van de meter vindt gecontroleerd plaats en de fysieke integriteit van de meter na installatie wordt gecontroleerd.	The installation of the meter is a controlled process, and the physical integrity of the meter after installation is checked.
5.1.0	Beheersmaatregel	De netbeheerder heeft procedures opgesteld en geïmplementeerd die waarborgen dat de installatie van de meter gecontroleerd plaats vindt en daarna de fysieke integriteit van de meter na installatie wordt gecontroleerd.	The grid operator has established and implemented procedures which guarantees that the installation of the meter is a controlled process, and next that is checked the physical integrity of the meter after the installation.
5.1.1	Implementatierichtlijn	Er wordt bij installatie gecontroleerd of de meter op het juiste adres staat.	Checking whether the meter is placed at the right address is part of the installation process.
5.1.2	Implementatierichtlijn	Er wordt bij installatie gecontroleerd of de elektriciteits- en gasmeter juist zijn gekoppeld.	During the installation is checked whether the electricity meter and gas meter are connected correctly.
5.1.3	Implementatierichtlijn	Er wordt bij installatie of deployment gecontroleerd dat de beveiligingsfunctionaliteit is ingeschakeld.	Checking that the security functionality is enabled, is part of the installation process.
5.1.4	Implementatierichtlijn	Er wordt bij installatie of deployment gecontroleerd of de meterinstellingen (tijd, datum, tarief) correct zijn ingesteld.	checking whether the meter settings time, date, price rates are set correctly, is part of the installation process.
5.2.0	Beheersmaatregel	Fysieke metercontrole dient in overeenstemming met de Meetcode opgenomen te zijn in de aansluit- en transport overeenkomst (ATO).	In accordance with the Meetcode (metering code) physical inspection of the meter will be part of the ATO (connection & transportation agreement)
6.0.0	Beheersdoelstelling	De netbeheerder zorgt ervoor dat systeemassets veilig worden vervangen en verwijderd, ook voor herplaatsen.	The grid operator ensures that system assets are safely removed and replaced, also for relocating.
6.1.0	Beheersmaatregel	De netbeheerder heeft procedures opgesteld en geïmplementeerd om afgedankte systeemassets waarop zich persoonsgegevens kunnen bevinden veilig te vernietigen.	The grid operator has established and implemented procedures for safely destroying end-of-life system assets, on which personal data can be found.
6.2.0	Beheersmaatregel	De netbeheerder heeft procedures opgesteld en geïmplementeerd om meters veilig te vervangen of te herplaatsen, zodoende de vertrouwelijkheid van gegevens in de meters te blijven waarborgen.	The grid operator has established and implemented procedures for replacing or relocating meters, that guarantee the confidentiality of data stored in the meters.
7.0.0	Beheersdoelstelling	Netbeheerder beheerst door middel van schriftelijke afspraken de relaties met derde partijen.	The grid operator controls by means of written agreements relationships with third parties.

7.1.0	Beheersmaatregel	Netbeheerder borgt door middel van contractuele afspraken dat leveranciers van diensten en producten geconstateerde beveiligingslekken en incidenten pro-actief melden en in overleg met de netbeheerder zo snel mogelijk oplossen. Hierbij wordt aangesloten bij het incidentmanagementproces van de netbeheerder.	The grid operator assures, through contractual arrangements with vendors / suppliers of services and products, that identified vulnerabilities and incidents are proactively reported and are solved in collaboration with the grid operator as soon as possible. The resolution of incidents will adhere to the incident management process of the grid operator.
7.2.0	Beheersmaatregel	Netbeheerder borgt dat iedere leverancier van systeemassets een schriftelijke verklaring oplevert dat zijn producten geen 'backdoors' bevatten waarmee ongeautoriseerd toegang tot de slimme-meterinfrastructuur kan worden verkregen.	The grid operator ensures that any vendor / supplier of system assets delivers a written statement, which determines that its products contain no backdoors, that make it possible to access unauthorised the advanced metering infrastructure.
7.3.0	Beheersmaatregel	Netbeheerder borgt dat alle leveranciers van producten en diensten meewerken aan audits door of namens de netbeheerder voor zover deze betrekking hebben op privacy- en informatiebeveiligingsaspecten van de slimme meterinfrastructuur.	The grid operator ensures that all vendors / suppliers of products and services contribute to audits by or on behalf of the grid operator, to the extent they relate to the privacy and information security aspects of the advanced metering infrastructure.
7.4.0	Beheersmaatregel	Netbeheerder borgt dat fabrikanten van systeemassets ten behoeve van het productieproces van deze assets adequate beveiligingsprocessen hebben vastgelegd en geïmplementeerd.	The grid operator ensures that manufacturers of system assets have formulated and implemented adequate security processes for production process of the system assets.
7.4.1	Implementatierichtlijn	Netbeheerders hebben schriftelijke afspraken met alle fabrikanten van systeemassets over generatie, installatie, opslag, verzending en verwijdering van sleutels en wachtwoorden. Onderdeel van de afspraken is dat fabrikanten alle door hen gegenereerde sleutels en wachtwoorden direct en voorgoed verwijderen uit alle systeemassets op aangeven van de netbeheerder.	The grid operators have written agreements with all manufacturers of system assets that cover the generation, installation, storage, sending (transportation) and disposal of keys and passwords. Part of the agreement is the instant and permanent removal of generated keys and passwords by the manufacture from any system asset, when so instructed by the grid operator.
7.5.0	Beheersmaatregel	Persoonsgegevens die worden verwerkt of die zijn bestemd om na doorgifte aan een derde land of een internationale organisatie te worden verwerkt, mogen slechts worden doorgegeven indien, onverminderd de overige bepalingen van deze verordening, de verwerkingsverantwoordelijke en de verwerker aan de in dit hoofdstuk neergelegde voorwaarden hebben voldaan; dit geldt ook voor verdere doorgiften van persoonsgegevens vanuit het derde land of een internationale organisatie aan een ander derde land of een andere internationale organisatie. Alle bepalingen van AVG artikel 44 en 45 worden toegepast opdat het door deze verordening voor natuurlijke personen gewaarborgde beschermingsniveau niet wordt ondermijnd.	Any transfer of personal data which are undergoing processing or are intended for processing after transfer to a third country or to an international organisation shall take place only if, subject to the other provisions of this Regulation, the conditions laid down in this Chapter are complied with by the controller and processor, including for onward transfers of personal data from the third country or an international organisation to another third country or to another international organisation. All provisions in GPDR article 44 and 45 shall be applied in order to ensure that the level of protection of natural persons guaranteed by this Regulation is not undermined.
7.5.1	Implementatierichtlijn	Netbeheerder draagt bij verwerking van persoonsgegevens buiten de EU zorg voor een overeenkomst, gebruik makende van de standaard EU modelcontracten en dient de netbeheerder jaarlijks vast te stellen of nog aan de voorschriften van de overeenkomst wordt voldaan.	In case of processing personal data outside the EU the grid operator ensures that there is a contract, which is using the standard EU model contracts, and the grid operator will monitor annually if the conditions in the agreement still are met.
8.0.0	Beheersdoelstelling	De beschikbaarheid, integriteit en vertrouwelijkheid van de encryptiesleutels worden beschermd door de netbeheerder.	The availability, integrity and confidentiality of the encryption keys are protected by the grid operator.

8.1.0	Beheersmaatregel	De netbeheerder borgt de beschikbaarheid, integriteit en vertrouwelijkheid van de encryptiesleutels. Bij encryptiesleutels die bekend zijn bij meterleveranciers borgt de netbeheerder dit contractueel.	The grid operator ensures the availability integrity and confidentiality of encryption keys. If the encryption keys are known to a supplier, the grid operator will be assure this through a contract.
8.2.0	Beheersmaatregel	De security sterkte van de gebruikte algoritmen binnen de slimme meterinfrastructuur (P0, P2, P3) is ten minste zo sterk als 128-bits AES voor meters met een maximale levensduur van 20 jaar. Cryptografische algoritmes kunnen symmetrisch of asymmetrisch zijn.	The security strength of algorithms applied within the advanced metering infrastructure is at least as strong as 128-bit AES for meters, with a maximum lifespan of 20 years. Cryptographic algorithms may be symmetrical or asymmetrical.
8.2.1	Implementatierichtlijn	Mede aan de hand van de prognose van NIST en/of ENISA wordt jaarlijks vastgesteld wat de minimale security strength (gebruikte algoritmen en sleutellengten) is voor meters en data routers. Voor meters en data routers waarvan de security strength na de jaarlijkse evaluatie lager uitkomt dan de minimale security strength op het moment van plaatsing, wordt mede aan de hand van ENISA (Algorithms, Key Sizes and Parameters Report recommendations) en/of NIST (Technical Report 800-57 part I) vastgesteld op welk moment vervanging (mogelijk alleen van de software) noodzakelijk is.	Partly on the basis of the forecast of NIST Technical Report 800-57 Part I, is set annually the minimum security strength (used algorithms and key lengths) for meters and 'data routers'. Meters and 'data routers' for which the security strength after the annual evaluation is lower than the minimum security strength at the time of placement, is set partly on the basis of NIST in Technical Report 800-57 part I at which time the replacement (possible, only the software) is necessary.
8.2.2	Implementatierichtlijn	Netbeheerder kan elk wachtwoord en elke gebruikte beveiligingssleutel in alle in de slimme-meterinfrastructuur voorkomende meters op afstand wijzigen. Niemand buiten de netbeheerder kan genoemde wachtwoorden en sleutels wijzigen.	The grid operator can change remotely any password and any security key, used in all of the advanced metering infrastructure present meters. No one outside the grid operator can change the mentioned passwords and keys.
8.2.3	Implementatierichtlijn	De zogenaamde 'master key' is uitgezonderd van de eis om sleutels op afstand te wijzigen, mits met deze sleutel niets in de meter te wijzigen is zonder ook een andere sleutel te kennen.	The so-called 'master key' is excluded from the requirement to change remotely the keys, provided that with this key nothing in the meter can be changed without knowing another key.
8.3.0	Beheersmaatregel	Netbeheerder heeft processen ten aanzien van sleutel- en wachtwoordbeheer vastgelegd en geïmplementeerd.	Grid operator has established and implemented processes regarding key and password management.
8.3.1	Implementatierichtlijn	Het importeren van initiële fabriekssleutels in de cryptoserver is enkel mogelijk via een beschreven en geïmplementeerd proces waarbij de beschikbaarheid, integriteit en vertrouwelijkheid van de fabriekssleutels gewaarborgd blijft.	Importing initial factory keys in the crypto server is only possible through a described and implemented process, whereby the availability, integrity and confidentiality of the factory keys is guaranteed.
8.3.2	Implementatierichtlijn	De cryptoserver voorziet in alle sleutelmanagement functionaliteiten: - Import van de initiële sleutels. - Sleutelgeneratie. - Sleutelvernieuwing. - Beveiligde (versleutelde) back-up. - Logging van handelingen met de sleutels. - DLMS Authenticatie van meters. - DLMS Encryptie en decryptie van berichten.	The crypto server provides all key management functions: - Import of the initial keys. - Key generation. - Key Renewal. - Secure (encrypted) backup. - Logging of operations with the keys. - DLMS Authentication of meters. - DLMS Encryption and decryption of messages.
8.3.3	Implementatierichtlijn	Om sleutels voldoende fysiek te beveiligen gebruikt de netbeheerder tenminste Hardware Security Modules (HSM) die gecertificeerd zijn volgens FIPS-140 2 Level 2 en/of Common Criteria EAL4+.	To physically secure the keys sufficient, the grid operator is using at least security modules that are certified according FIPS-140 2 Level 2 and / or Common Criteria EAL4 +.

8.3.4	Implementatierichtlijn	Bij het genereren van sleutels door de cryptoserver wordt gebruik gemaakt van een gevalideerde random number generator volgens RNGVS.	When generating keys by the crypto server, will be used a validated random number generator according RNGVS.
8.3.5	Implementatierichtlijn	Sleutels zijn alleen binnen de cryptoserver unencrypted beschikbaar.	Keys are only unencrypted available within the crypto server.
8.3.6	Implementatierichtlijn	Er vindt na deployment geen meteranalyse in het veld plaats via de P0-poort met unencrypted sleutels.	After deployment there is not executed a meter analysis through the P0-port, with unencrypted keys.
9.0.0	Beheersdoelstelling	Privacygevoelige informatie uit en naar de meter dient end-to-end zodanig beveiligd te zijn dat integriteit en vertrouwelijkheid gewaarborgd blijft. De P1-poort is uitgezonderd zolang dit een alleen-lezenpoort betreft.	Privacy sensitive information from and to the meter should always remain end-to-end secured, that integrity and confidentiality are guaranteed. The P1 port is excluded as long this is a read-only port.
9.1.1	Implementatierichtlijn	Hierbij geldt dat data routers versleutelde berichten met meetgegevens die tussen het centraal systeem en meters verzonden worden niet kunnen ontsleutelen; dergelijke berichten worden versleuteld doorgezonden. Metergegevens, niet zijnde meetgegevens kunnen door de data routers worden ontsleuteld.	Whereby applies that data routers can not decrypt the encrypted messages with measurement data that are transmitted between the central system and meters; such messages are sent encrypted. Meter data, other than measurement data, can be decrypted by the data routers.
9.2.0	Beheersmaatregel	- De privacy gevoelige informatie in de slimme meterinfrastructuur is, minimaal op applicatieniveau, van de meter tot de centrale P4 beveiligd tegen aanvallen op vertrouwelijkheid en integriteit. - Op communicatieniveau worden maatregelen getroffen om de integriteit (en de beschikbaarheid) van de onderliggende IT-voorzieningen en netwerken als WAN, GPRS, CDMA, PLC te waarborgen.	- The privacy-sensitive information in the advanced metering infrastructure is, at least at the application level of the meter to the central P4 protected against attacks on confidentiality and integrity. - At the communication level, measures are taken to protect integrity (and availability) of the underlying IT facilities en networks like WAN, GPRS, CDMA, PLC.
9.2.1	Implementatierichtlijn	Hierbij geldt dat het technisch onmogelijk is om met de meter over genoemde informatietypes te communiceren buiten de gedefinieerde end-to-end beveiligde kanalen.	Whereby applies that it is technically impossible to use the meter for mentioned information types to communicate outside the defined end-to-end secured channels.
9.3.0	Beheersmaatregel	Alle communicatie vanaf de meter dient beveiligd te zijn zodat beschikbaarheid, integriteit en vertrouwelijkheid van berichten is gewaarborgd.	All communications from the meter must be protected so that availability, integrity and confidentiality of messages are guaranteed.
9.3.1	Implementatierichtlijn	Hierbij geldt dat voor encryptie van communicatie per communicatiekanaal unieke sleutels worden gebruikt.	Whereby applies that for encryption of communication per communication channel unique keys are used.
9.4.0	Beheersmaatregel	Het meerdere malen versturen van hetzelfde bericht dient niet te mogen leiden tot het meer dan eenmaal accepteren van dat bericht (‘replay attacks’).	Repeatedly sending the same message should not result in more than one acceptance of the same message ("replay attacks").
10.0.0	Beheersdoelstelling	De netbeheerder beheerst wijzigingen in de slimme-meterinfrastructuur.	The grid operator controls changes in the advanced metering infrastructure.
10.1.0	Beheersmaatregel	Binnen de netbeheerder dient een proces voor wijzigingsbeheer voor systeemassets binnen de slimme-meterinfrastructuur te zijn vastgelegd en geïmplementeerd.	Within the grid operator, a process should be established and implemented for change management of system assets within the advanced metering infrastructure.
10.1.1	Implementatierichtlijn	Hierbij geldt dat wijzigingsbeheerprocedures dienen te worden verwerkt in het kwaliteitsbeheersysteem van de netbeheerder.	Hereby applies that change management procedures should be included in the quality management system of the grid operator.
10.2.0	Beheersmaatregel	Alle wijzigingen aan gegevens in het centraal systeem dienen te worden gelogd.	All changes to data in the central system should be logged.
10.2.1	Implementatierichtlijn	Logging moet altijd naar unieke personen zijn te herleiden.	Logging should always be traced back to uniquely identifiable persons
10.2.2	Implementatierichtlijn	Logging moet altijd read only zijn.	Logging should always be read only.

10.3.0	Beheersmaatregel	Netbeheerders dienen een configuratiemanagementproces te hebben geimplementeerd.	Grid operators should have implemented a configuration management process
10.3.1	Implementatierichtlijn	Als onderdeel van het configuratiemanagementproces hebben de Netbeheerders een actueel overzicht van de systeemassets die aanwezig zijn binnen de slimme-meterinfrastructuur.	Grid operators have an overview of the system assets present in the advanced metering infrastructure as part of the configuration management process.
10.3.2	Implementatierichtlijn	Het actuele overzicht van systeemassets bevat ten minste de volgende onderdelen: Van meters: - Identifier. - Fabrikant en type. - Softwareversie. - Meterconfiguratie. Specifiek van het centraal systeem: - Architectuuroverzicht. Daarnaast is van de gehele slimme-meterinfrastructuur een overzicht beschikbaar met systeemassets en de koppelingen daartussen.	The overview of system assets includes at least the following components: Of meters: - Identifier. - Manufacturer and type. - Software version. - Meter configuration. Specific for the central system: - Architecture Overview. Additionally, there is available an overview of the entire advanced metering infrastructure with its system assets and the interfaces between them.
10.4.0	Beheersmaatregel	Wanneer een nieuwe verwerking van slimme meter gegevens (persoonsgegevens), gelet op de aard, de omvang, de context en de doeleinden daarvan waarschijnlijk een hoog risico inhoudt voor de rechten en vrijheden van natuurlijke personen voert de verwerkingsverantwoordelijke (Netbeheerder) eenmalig vóór de verwerking een beoordeling uit van het effect van de beoogde verwerkingsactiviteiten op de bescherming van persoonsgegevens (DPIA).	If a new processing of smart meter data (personal data) is likely to pose a high risk to the rights and freedoms of natural persons due to the nature, size, context and purposes thereof, the controller (grid operator) will perform a one-off pre-processing assessment of the impact of the intended processing activities on the protection of personal data (DPIA).

10.5.0	Beheersmaatregel	1. Rekening houdend met de stand van de techniek, uitvoeringskosten, aard, omvang, context en het doel van de verwerking alsook met de qua waarschijnlijkheid en ernst uiteenlopende risico's voor de rechten en vrijheden van natuurlijke personen welke aan de verwerking zijn verbonden, treft de verwerkingsverantwoordelijke, zowel bij de bepaling van de verwerkingsmiddelen als bij de verwerking zelf, passende technische en organisatorische maatregelen, zoals pseudonimisering, die zijn opgesteld met als doel de gegevensbeschermings-beginselen, zoals minimale gegevensverwerking, op een doeltreffende manier uit te voeren en de nodige waarborgen in de verwerking in te bouwen ter naleving van de voorschriften van de AVG en ter bescherming van de rechten van de betrokkenen. 2. De verwerkingsverantwoordelijke treft passende technische en organisatorische maatregelen om ervoor te zorgen dat in beginsel alleen persoonsgegevens worden verwerkt die noodzakelijk zijn voor elk specifiek doel van de verwerking. Die verplichting geldt voor de hoeveelheid verzamelde persoonsgegevens, mate waarin zij worden verwerkt, termijn waarvoor zij worden opgeslagen en toegankelijkheid daarvan. Deze maatregelen zorgen met name ervoor dat persoonsgegevens in beginsel niet zonder menselijke tussenkomst voor een onbeperkt aantal natuurlijke personen toegankelijk worden gemaakt. 3. Overeenkomstig AVG artikel 42 kan een netbeheerder ervoor kiezen om via een goedgekeurde certificering aan te tonen dat aan de voorschriften van 1 en 2 is voldaan.	1. Taking into account the state of the art, implementation costs, nature, scope, context and purpose of the processing, as well as the risks and risks of the rights and freedoms of natural persons associated with processing in terms of probability and severity, the controller, both in the determination of the processing means and in the processing itself, appropriate technical and organizational measures, such as pseudonymisation, which have been drawn up with the aim of implementing the data protection principles, such as minimal data processing, in an effective manner and the necessary safeguards to be incorporated in the processing in order to comply with the regulations of the GPDR and to protect the rights of the data subjects. 2. The controller shall take appropriate technical and organizational measures to ensure that in principle only personal data are processed that are necessary for each specific purpose of the processing. This obligation applies to the amount of collected personal data, the extent to which they are processed, the period for which they are stored and access to them. In particular, these measures ensure that personal data are in principle not made available to an unlimited number of natural persons without human intervention. 3. In accordance with GPDR article 42, a network operator may choose to demonstrate compliance with the requirements of 1 and 2 by means of an approved certification.
11.0.0	Beheersdoelstelling	De netbeheerder borgt dat kleinverbruikers en marktpartijen kunnen vertrouwen op de meterstanden van de meter.	The grid operator ensures that private consumers and market participants can rely on the measurement data of the meter.
11.1.0	Beheersmaatregel	De instellingen van het metrologische gedeelte van de meter en alle in het metrologisch gedeelte opgeslagen informatie, waaronder meetstanden, dienen na levering aan de netbeheerder niet aangepast te kunnen worden.	The settings of the metrological part of the meter, and all in the metrological part stored information, including measurement data, should not be adjustable after delivery to the grid operator.
11.2.0	Beheersmaatregel	Geregistreerde meterstanden in het centraal systeem dienen niet te kunnen worden gewijzigd.	Registered measurement data in the central system cannot be modified.
11.2.1	Implementatierichtlijn	Hierbij geldt dat het centraal systeem een herstelmogelijkheid dient te hebben in geval van bijzondere situaties, zoals uitval van de database.	Whereby applies that the central system should have a recovery possibility in case of special circumstances, such as failure of the database.
11.2.2	Implementatierichtlijn	De beveiliging van de back up van informatie uit de slimme-meterinfrastructuur mag niet lager zijn dan van de beveiliging van de productiegegevens.	In the advanced metering infrastructure the security of back-up data cannot be lower than the security of the original production data.
11.3.0	Beheersmaatregel	De netbeheerder borgt dat de tijdsafwijking in de slimme meterinfrastructuur acceptabel is.	The grid operator ensures that time differences operate within acceptable boundaries.

11.3.1	Implementatierichtlijn	De netbeheerder borgt dat de tijdsafwijking van de tijd in het centraal systeem zoals gebruikt voor tijdsynchronisatie acceptabel is vergeleken met een vastgestelde, onafhankelijke bron (Network Time Protocol - NTP).	The grid operator ensure that the time stamp of the Central System used for time synchronization, is itself synchronised with a determined independent source (Network Time Protocol - NTP)
11.3.2	Implementatierichtlijn	De netbeheerder borgt dat de elekriciteitsmeter een tijdsafwijking heeft die niet groter is dan een halve seconde per 24 uur.	The grid operator assures that the E-meter does not have a time deviation larger than half a second every 24 hours.
11.3.3	Implementatierichtlijn	De netbeheerder borgt dat de gasmeter een tijdsafwijking heeft die niet groter is dan 10 seconden per 24 uur.	The grid operator assures that a G-meter does not have a time deviation larger than 10 seconds every 24 hours.
11.3.4	Implementatierichtlijn	Hierbij geldt dat de mogelijke tijdsafwijking op de elektriciteitsmeters en de gasmeters periodiek dienen te worden gecontroleerd en, indien nodig, bij afwijking worden gerapporteerd. Indien afwijkingen structureel blijken te zijn, dient er nader onderzoek te worden verricht.	Periodic checking of time discrepancies and reporting of anomalies is mandatory. Structural discrepancies warrant further investigation.
12.0.0	Beheersdoelstelling	Toegang tot het datacommunicatienetwerk is voldoende veilig ingericht.	Access to the data communication network is set up sufficiently secure.
12.1.0	Beheersmaatregel	Opslag van logingegevens voor geautomatiseerde toegang tot een datacommunicatienetwerk dient alleen in het meter of data routers plaats te vinden.	Storage of login data for automated access to a data communication network should only occur in the meter or data router.
12.1.1	Implementatierichtlijn	In het geval van gebruik van een SIM-kaart voor GPRS en LTE of R-UIM voor CDMA t.b.v. identificatie geldt dat APN-logingegevens nooit op de SIM-kaart mogen worden geplaatst en Domein-inloggegevens niet op de R-UIM.	In case of using a SIM card in case of GPRS and LTE or R-UIM in case of CDMA for identification, applies that APN login data are never placed on the SIM card and Domain inlog data on the R-UIM.
12.2.0	Beheersmaatregel	In het geval de datacommunicatie met behulp van een SIM-kaart of R-UIM wordt opgebouwd, dienen maatregelen getroffen te zijn om de koppeling tussen SIM-kaart of R-UIM en communicatiemodule te controleren en in stand te houden.	In case of data communication with the aid of a SIM card or R-UIM is build up, measures should be taken to monitor and maintain the link between the SIM card or R-UIM and the communication module.
12.2.1	Implementatierichtlijn	Om te controleren of sprake van een juiste koppeling is dient de datacommunicatieleverancier te controleren dat de SIM-kaart of R-UIM geïnstalleerd is in een apparaat uit de juiste reeks modemnummers (IMEI-nummers respectievelijk ESN).	To be able to check if there is a proper link, the data communication provider should verify that the SIM card or R-UIM is installed in a device from the right set of modem numbers (IMEI numbers or ESN).
12.2.2	Implementatierichtlijn	Om de koppeling in stand te houden geldt dat: - of de SIM-kaart / R-UIM is verlijmd met de communicatiemodule; - of de SIM-kaart / R-UIM zodanig is ingesteld dat deze, na in het ene apparaat gebruikt te zijn, nooit meer in een ander apparaat gebruikt kan worden; - of datacommunicatieleveranciers SIM-kaarten/ R-UIM blokkeren als deze geplaatst zijn buiten een bepaalde set van modemnummers of als er misbruik van de SIM-kaarten/R-UIM wordt geconstateerd.	In order to maintain the link, applies that: - Or the SIM card / R-UIM is glued to the communication module; - Or the SIM card / R-UIM is set in a way which, after the SIM card is used in one device, it never can be used in another device; - Or data communication providers lock the SIM card / R-UIM if this is placed outside a certain set of modem numbers.
12.3.0	Beheersmaatregel	In het geval van een SIM/UIM-loze oplossing moeten de gebruikersnaam en het wachtwoord voor toegang tot het CDMA/GPRS/LTE-netwerk beveiligd opgeslagen zijn op het modem.	In case of a SIM / UIM-free solution, the user name and password to access the CDMA / GPRS / LTE network should be securely stored on the modem.
12.3.1	Implementatierichtlijn	De gebruikersnaam en het wachtwoord moeten versleuteld worden opgeslagen.	The username and password must be stored encrypted.

12.4.0	Beheersmaatregel	De netbeheerder borgt dat datacommunicatieleveranciers de toegang tot een (deel van een) netwerk tot enkel en alleen de afnemende netbeheerder beperken (exclusieve toegang, zoals een 'private APN' in GPRS en LTE en 'Domein' in CDMA).	The grid operator ensures that data communication providers restrict the access to (a segment of) the grid exclusively to the purchasing grid operator (exclusive access like the private APN for GPRS and LTE and the domain for CDMA).
12.5.0	Beheersmaatregel	De netbeheerder borgt dat datacommunicatieleveranciers de toegang tot diensten, netwerkpoorten en systemen beperken tot wat noodzakelijk is voor het functioneren van de slimme-meterinfrastructuur.	The grid operator ensures that data communication providers are limiting the access to services, network ports and systems to what is necessary for operating the advanced metering infrastructure.
12.6.0	Beheersmaatregel	De netbeheerder borgt dat datacommunicatieleveranciers procedures hebben gedefinieerd, vastgelegd en geïmplementeerd om in geval van calamiteiten het deel van het datacommunicatienetwerk gebruikt voor de slimme-meterinfrastructuur snel te kunnen afschakelen.	The grid operator ensures that data communication providers have described and implemented procedures to disable the datacom network that is used in the smart metering infrastructure in the case of calamities.
12.7.0	Beheersmaatregel	De netbeheerder borgt door middel van contractuele afspraken dat de datacommunicatieleverancier tijdig met de netbeheerder overlegt over toekomstige wijzigingen in de communicatiefunctie. Hierbij wordt rekening gehouden met de levensduur van deze functionaliteit.	The grid operator contractually binds the datacom provider for timely consultation concerning future changes in the communication functionality. The life span of this functionality is taken into account.
12.8.0	Beheersmaatregel	De netbeheerder legt contractueel vast dat datacommunicatieleveranciers netwerkbeveiligingsmaatregelen hebben getroffen om de beveiliging en privacy van de slimme-meterinfrastructuur te waarborgen.	The grid operator will contractually bind the data communication providers to appropriate network security measures for the privacy and security of the advanced metering infrastructure.
12.8.1	Implementatierichtlijn	Zowel preventieve als detectieve maatregelen worden getroffen om communicatienetwerken te beveiligen, waaronder in elk geval: - firewalls om de netwerkinfrastructuur bij de datacommunicatieleverancier te beschermen. - waar relevant het installeren van anti-virussoftware. - waar relevant logging en monitoring door middel van Intrusion Detection Systems of Intrusion Prevention Systems.	Both preventive and detective measures are taken to secure communication networks, including in any case: - Firewalls to protect the network infrastructure at the data communications provider. - Where relevant, the installation of anti-virus software. - Where relevant, logging and monitoring by means of Intrusion Detection Systems or Intrusion Prevention Systems.
12.9.0	Beheersmaatregel	Datacommunicatie verloopt alleen over ten minste logisch gescheiden verbindingen voor de gedefinieerde end-to-end beveiligde routes.	Data communication only takes place at least on connections that are at least logically separated for the defined end-to-end secured routes.
12.9.1	Implementatierichtlijn	De netbeheerder dient te borgen dat datacommunicatieleveranciers geen communicatie mogelijk maakt tussen meters.	The grid operator ensures that datacom suppliers do not enable communication between meters directly.
12.10.0	Beheersmaatregel	Communicatie over de P0-, P2-, P3- en P4-poorten is beveiligd, zodanig dat beschikbaarheid, integriteit, en vertrouwelijkheid beschermd worden. De P1-poort is uitgezonderd zolang dit een alleen-lezenpoort betreft.	Communication on the P0-, P2-, P3- and P4-ports is protected, such that availability, integrity, and confidentiality are protected. The P1-port is excluded, as long as it is a read-only port.
12.10.1	Implementatierichtlijn	Ter controle van correctheid geldt dat de meter geen communicatie buiten een per poort gedefinieerde, beperkte set van toegestane berichten accepteert.	To check the accuracy, applies that the meter accepts no communication outside a per port defined, limited set of allowable messages.

13.0.0	Beheersdoelstelling	De slimme-meterinfrastructuur is voldoende beschermd tegen externe verstoringen.	The advanced metering infrastructure is adequately protected against external disruptions.
13.1.0	Beheersmaatregel	De netbeheerder dient de P3- en P4-poort te beveiligen tegen aanvallen, waaronder Denial of Service-aanvallen (DoS-Aanvallen), en maatregelen te treffen die de gevolgen van aanvallen minimaliseren.	The grid operator should protect the P3- and P4-port against attacks, including Denial of Service attacks, and to take measures to limit the effects of attacks.
13.1.1	Implementatierichtlijn	Tegen Denial of Service-aanvallen (DoS-Aanvallen) kan geregeld worden dat IP-ranges bij de Internet Service Provider geblokkeerd kunnen worden en dat SIM-kaarten / R-UIM bij de datacommunicatieleverancier geblokkeerd kunnen worden. Er wordt rekening gehouden met de volgende typen aanvallen: - Aanvallen op bandbreedte van het netwerk. - Aanvallen gericht op systemen binnen het netwerk. - Aanvallen op specifieke operating systems. - Aanvallen op protocoleigenschappen. - Aanvallen gericht op specifieke applicaties.	Against Denial of Service attacks it can be arranged that IP-ranges at the Internet Service Provider can be blocked, and that SIM cards / R-UIM at data communication provider can be blocked. It takes into account the following types of attacks: - Attacks on network bandwidth. - Attacks aimed at systems within the network. - Attacks on specific operating systems. - Attacks on protocol properties. - Attacks aimed at specific applications.
13.1.2	Implementatierichtlijn	Aanvallen op beschikbaarheid van de P3-poort van de meter met gebruikersnaam en wachtwoord moeten worden gepareerd ('DoS attack'). Tijdelijk lock-out mechanisme moet voorkomen dat op grote schaal meters in het netwerk voor langere tijd niet bereikbaar zijn.	DoS attacks on the P3-port using user-id and password must be blocked. Temporary lock-out mechanisms should prevent prolonged unavailability of meters in the grid on a larger scale.
13.2.0	Beheersmaatregel	De netbeheerder dient te monitoren dat meters en data routers bereikbaar zijn.	The grid operator should monitor the accessibility of meters and data routers.
13.2.1	Implementatierichtlijn	Het centraal systeem genereert een waarschuwing als een meter of data routers langer dan een vastgestelde termijn niet bereikt kan worden na een periodiek uitleesmoment. De vastgestelde termijn is ten hoogste tien kalenderdagen.	The central system generates a warning if a meter or data router can not be reached longer than a specified period after a periodic read out moment of the meter. The specific period (deadline) is maximally ten calendar days.
15.0.0	Beheersdoelstelling	De netbeheerder beheerst de software op meters.	The grid operator controls the software on meters.
15.1.0	Beheersmaatregel	De netbeheerder kan kritieke beveiligingsfunctionaliteit van geïnstalleerde meters snel en veilig updaten, waarbij de netbeheerder een impactanalyse uitvoert die mede bepaalt welke termijn wordt gehanteerd.	The grid operator can quickly and safely update critical security functionality of installed meters. To do so the grid operator performs an impact analysis assisting in the determination of the timing and frequency of such updates.
15.1.1	Implementatierichtlijn	Componenten in de meter die software bevatten zijn voldoende beveiligd op vertrouwelijkheid en integriteit. Dit betekent dat de beheerdersinterface (JTAG) voor de software in de meter dicht staat of is beveiligd.	Components in the meter containing software are sufficient secured for (protecting) confidentiality and integrity. This means that the maintenance interface (JTAG) is disabled or is secured.
15.1.2	Implementatierichtlijn	Software wordt alleen geaccepteerd wanneer deze afkomstig is van een geauthenticeerde partij.	Software will only be accepted if it originates from an authenticated party.
15.2.0	Beheersmaatregel	Netbeheerder borgt dat de softwareversie en aanwezige beveiligingsfunctionaliteit op meters regelmatig gecontroleerd worden.	The grid operator ensures that regularly is checked the software versions and present security functionality of meters.

15.2.1	Implementatierichtlijn	De netbeheerder borgt dat het technisch mogelijk is om softwareversies en aanwezige beveiligingsfunctionaliteit, waaronder relevante configuratiegegevens, in de slimme-meterinfrastructuur op te vragen en te controleren.	The grid operator ensures that it is technically possible to query and check the software versions and present security functionality, including relevant configuration data in the advanced metering infrastructure.
15.4.0	Beheersmaatregel	Voordat softwareupdates worden geïnstalleerd, doorlopen deze een vastgesteld testproces. Bij een negatieve uitkomst van de uitgevoerde tests worden tekortkomingen in de softwareupdate verholpen vóór installatie van de update.	Before software updates are installed, they will follow an established testing process. In case of a negative outcome of the performed tests, the shortcomings in the software update are corrected before installing the update.
16.0.0	Beheersdoelstelling	Netbeheerders leggen in overeenkomsten met leveranciers van diensten en producten een acceptabel beveiligingsniveau vast.	The grid operator will record acceptable security levels for products and services in binding contracts with vendors / suppliers.
16.1.0	Beheersmaatregel	Netbeheerder borgt dat installatiebedrijven pas met meters en data routers werken als zij aan kunnen tonen een voldoende beveiligingsniveau te realiseren in lijn met het beveiligingsniveau van de netbeheerder.	The grid operator ensures that installation companies only can work with meters and data routers, after they have demonstrated that they are realising an adequate level of security complying to security demands of the grid operator.
16.1.1	Implementatierichtlijn	De volgende maatregelen maken deel uit van de schriftelijke afspraken tussen de netbeheerder en de installatiebedrijven: - het installatiebedrijf tekent een bewerkersovereenkomst. - het installatiebedrijf verklaart in de bewerkersovereenkomst met de netbeheerder dat het installatiebedrijf vertrouwelijk omgaat met privacygevoelige informatie. - privacygevoelige informatie wordt vernietigd na gebruik, of zo gauw de netbeheerder daar om vraagt. - netbeheerder heeft recht tot audit om (steekproefsgewijs) te controleren of installatiebedrijven en monteurs werken volgens de Eisen privacy en security van de slimme-meterinfrastructuur en het beveiligingsbeleid van de netbeheerder. De netbeheerder maakt ten minste gebruik van dit recht bij vermoedens van niet handelen conform afspraken.	The following measures are part of the written agreements between the grid operator and the installation companies: - The installation company signs a data processing agreement. - The installation states in the data processing agreement with the grid operator that the installation company will handle sensitive information confidential. - Privacy-sensitive information is destroyed after use, or as soon as the grid operator asks for it. - The grid operator has the right to audit and (at random) to check if installation companies and their mechanics work accordingly to the Dutch Requirements for Privacy and Security of the Advanced Metering Infrastructure and security policy of the grid operator itself. The grid operator makes at least use of this right in case of suspicions of not acting in accordance with the agreements.
16.2.0	Beheersmaatregel	In overeenkomsten met leveranciers van producten en diensten wordt vastgelegd dat de in de praktijk toegepaste beveiligingsoplossingen door instanties, in opdracht van de netbeheerder, kunnen worden beoordeeld. Daarbij is er geen sprake van geheimhouding van ontwerp of broncode van (onderdelen van) de in de praktijk toegepaste beveiligingsoplossingen.	Allowing and enabling the assessment of realized and operational security solutions is a part of the contract between grid operator and suppliers of products and services. For the assessment of such operational security solutions by the grid operator or third parties designated by the grid operator, the supplier cannot refer to non-disclosure agreements or secrecy clauses.
16.2.1	Implementatierichtlijn	De gebruikte cryptografische technieken zijn alleen op publiek beschikbare standaarden (zoals NIST of IEEE) gebaseerd en de techniek is breed getoetst en geaccepteerd.	The used cryptographic techniques are only based on publicly available standards (like NIST or IEEE) and the technique has been widely tested and accepted.
17.0.0	Beheersdoelstelling	Netbeheerders hebben controle over Portal-P4.	Grid operators control Portal-P4.
17.1.0	Beheersmaatregel	Netbeheerders moeten zeker stellen dat een Energieleverancier of ODA die van Portal-P4 gebruik wil maken opereert conform wet- en regelgeving.	Grid operators must ensure that Energy Suppliers or Independent Third Parties (ODA) operate in accordance with legislation and regulation when utilizing Portal-P4.

17.1.1	Implementatierichtlijn	Een Energieleverancier of ODA die van Portal-P4 gebruik wil maken, heeft vooraf een directieverklaring getekend.	Any E-supplier or ODA will have signed a management statement by a member of the executive board prior to utilizing Portal-P4.
17.2.0	Beheersmaatregel	Een Energieleverancier of ODA die van Portal-P4 gebruik wil maken, dient daarvoor een technische validatie uit te voeren op de juiste toepassing van het beveiligingscertificaat, het protocol en de berichtendefinitie. Het succesvol doorlopen van de validatie leidt tot toegang tot de Portal-P4. EDSN is verantwoordelijk voor deze validatie.	In order to utilize Portal-P4 an E-supplier or ODA must perform a technical validation to assess the correct application of the security certificate, the protocol and the message definition. A successful validation grants access to the Portal-P4. EDSN is responsible for this validation.
17.3.0	Beheersmaatregel	Netbeheerders mogen bij redelijke vermoedens van misbruik de toegang tot Portal-P4 (tijdelijk) intrekken. Zij melden dit met een motivatie aan de betreffende Energieleverancier of ODA.	In case of reasonable suspicion of abuse the grid operator can (temporarily) revoke access rights to Portal-P4. These actions will be reported to the E-supplier or ODA concerned including the motivation.
17.3.1	Implementatierichtlijn	Netbeheerders kunnen toegang tot Portal-P4 intrekken: bij geconstateerd misbruik door Energieleverancier of ODA; als een Energieleverancier opvragingen doet die niet overeenkomen met de eigen aansluitingen; als een ODA lijsten met klantmandaten niet vooraf oplevert; en als een ODA opvragingen doet die niet overeenkomen met lijsten met de klantmandaten.	Grid operators can revoke access to Portal-P4: - in case of abuse by E-supplier or ODA - if and when an E-supplier performs queries outside their own connection base - if and when an ODA does not provide the required lists with consumer mandates - if and when an ODA performs queries outside their own set of mandates.
17.3.2	Implementatierichtlijn	EDSN kan op verzoek van Netbeheerders de toegang tot de P4 poort intrekken.	EDSN can revoke access to the P4 port at the request of the grid operator.
17.3.3	Implementatierichtlijn	Een geconstateerd misbruik op Portal-P4-poort wordt beschouwd als een incident. Een incident worden geregistreerd in het sectorbrede incidentenregister van de Netbeheerders.	Observed abuse of Portal-P4 is considered an incident. Incidents will be recorded in the grid operator's sector-wide incident register.
17.4.0	Beheersmaatregel	Het Centraal Systeem (CS) van een Netbeheerder dient op Portal-P4 alleen communicatie van Energieleveranciers, Gas Netbeheerders en ODA’s te accepteren.	The Central System (CS) of grid operators should only accept messages in Portal-P4 from E-suppliers, G-suppliers and ODA's.
17.5.0	Beheersmaatregel	Het Centraal Systeem (CS) van een Netbeheerder dient alleen opvragingen van een Energieleverancier over Portal-P4 te accepteren als deze opvragingen overeenkomen met de aansluitingen van de Energieleverancier.	The CS should only accept requests in Portal-P4 by an E-supplier if such request is in accordance with that E-supplier's set of connections.
17.5.1	Implementatierichtlijn	Er moet worden gecontroleerd of de opvragingen van een Energieleverancier overeenkomen met de opgegeven aansluitingen in het C-AR.	Requests by E-suppliers will be matched against the registered connections in the C-AR.
17.6.0	Beheersmaatregel	Het Centraal Systeem (CS) van een Netbeheerder dient alleen opvragingen van een ODA over Portal-P4 te accepteren als deze opvragingen overeenkomen met de vooraf ingeleverde lijsten met klantmandaten van de ODA.	The CS should only accept requests in Portal-P4 by an ODA if such request is in accordance with that ODA's pre-handed list of consumer mandates.
17.6.1	Implementatierichtlijn	Een ODA dient vooraf lijsten met aansluitingen op te leveren waarvoor zij klantmandaten hebben ontvangen. Voor deze aansluitingen kunnen metergegevens via Portal-P4 bij netbeheerders worden opgevraagd.	An ODA will pro-actively hand in lists with connections with consumer mandates. For these connections metering data can be requested from grid operators through Portal-P4.

17.7.0	Beheersmaatregel	De toegestane communicatie met Energieleveranciers en ODA's dient zich te beperken tot wat in de BRS-P4 is vastgelegd.	Mandated communication with E-suppliers and ODA's must be restricted in accordance with the specifications of BRS-P4.
17.8.0	Beheersmaatregel	EDSN fungeert alleen als doorgeefluik voor de meetgegevens. EDSN slaat alleen gedurende een beperkte tijd (nodig voor het garanderen van het beantwoorden van de P4 dataverzoeken van LV en ODA) meetgegevens op.	EDSN acts as an interface between the grid operators and the market parties. EDSN will only store metering data (necessary for guaranteed responding to P4 data requests of supplier and ODA) for a limited duration.
G1.0.0	Beheersdoelstelling	1.Persoonsgegevens moeten: a)worden verwerkt op een wijze die ten aanzien van de betrokkene rechtmatig, behoorlijk en transparant is („rechtmatigheid, behoorlijkheid en transparantie”); b) voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden worden verzameld en mogen vervolgens niet verder op een met die doeleinden onverenigbare wijze worden verwerkt; de verdere verwerking met het oog op archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden wordt overeenkomstig artikel 89, lid 1, niet als onverenigbaar met de oorspronkelijke doeleinden beschouwd („doelbinding”); c) toereikend zijn, ter zake dienend en beperkt tot wat noodzakelijk is voor de doeleinden waarvoor zij worden verwerkt („minimale gegevensverwerking”); 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) worden bewaard in een vorm die het mogelijk maakt de betrokkenen niet langer te identificeren dan voor de doeleinden waarvoor de persoonsgegevens worden verwerkt noodzakelijk is; persoonsgegevens mogen voor langere perioden worden opgeslagen voor zover de persoonsgegevens louter met het oog op archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden worden verwerkt overeenkomstig artikel 89, lid 1, mits de bij deze verordening vereiste passende technische en organisatorische maatregelen worden getroffen om de rechten en vrijheden van de betrokkene te	1. Personal data shall be: (a) processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency'); (b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation'); (c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation'); (d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy'); (e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation'); (f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures
G1.1.0	Beheersmaatregel	De Netbeheerder houdt zich aan alle onderdelen van de sectorbrede zelfregulering van de Privacy en Security slimme-meterinfrastructuur en de Gedragscode.	The grid operator complies to all aspects of the sector-wide self regulation of the Privacy and Security of the advanced metering infrastructure and the Code of Conduct.
G1.2.0	Beheersmaatregel	Naast de kaders van de wet en de sectorbrede zelfregulering, dient de Netbeheerder een privacy- en informatiebeveiligingsbeleid hebben, waarin het beleid van de betreffende Netbeheerder ten aanzien van de Verwerking en bescherming van Persoonsgegevens nader is geregeld.	Besides the frameworks provided by law, self regulation agreements and code of conduct, the grid operator must have a privacy & information security policy in place that covers the processing and protection of Personal Data.

G1.2.1	Implementatierichtlijn	Alle medewerkers van de netbeheerder die gegevens verwerken uit de slimme meterinfrastructuur dienen op de hoogte te zijn van de kaders van de geldende wet- en regelgeving.	All grid operator personnel processing data from the advanced metering infrastructure must be aware of the guidelines provided by law and regulations.
G1.2.2	Implementatierichtlijn	De netbeheerder voert een risicomanagementcyclus uit, waarbinnen rekening wordt gehouden met nieuwe en bestaande risico's, kwetsbaarheden en incidenten. De netbeheerder voert een periodieke risicoanalyse uit om te verzekeren dat juiste en volledige maatregelen voor gecontroleerd beheer zijn geïdentificeerd, goedgekeurd en geïmplementeerd. Op basis hiervan worden ook reeds bestaande maatregelen aangepast aan de geconstateerde risico's en aanvullende maatregelen getroffen.	The grid operator shall perform a risk management cycle addressing new and existing risks, vulnerabilities and incidents. The grid operator will execute periodic risk assessments to ensure that accurate and complete measures for risk mitigation have been identified approved and implemented. Following the assessment outcome existing measures can be updated and additional measures implemented.
G1.2.3	Implementatierichtlijn	De netbeheerder dient het eigen privacy- en informatiebeveiligingsbeleid ten minste jaarlijks en zodra zich belangrijke ontwikkelingen voordoen, te beoordelen en wanneer nodig bij te stellen om te zorgen dat het geschikt, toereikend en doeltreffend blijft.	To ensure that privacy and information security policies remain appropriate, sufficient and effective the grid operator will review and adjust such policies at least once a year and whenever major developments warrant it.
G1.2.4	Implementatierichtlijn	De netbeheerder maakt daarnaast een planning voor het uitvoeren van penetratietesten om kwetsbaarheden binnen de slimme-meterinfrastructuur te identificeren. Op basis hiervan worden ook reeds bestaande maatregelen aangepast aan de geconstateerde risico's en aanvullende maatregelen getroffen.	The grid operator will also plan and execute penetration tests to identify vulnerabilities in the advanced metering infrastructure. Following the test outcome existing measures can be updated and additional measures implemented.
G1.2.5	Implementatierichtlijn	De netbeheerder heeft het risicomanagementproces gekoppeld aan het incidentmanagementproces. Op basis hiervan worden ook reeds bestaande maatregelen aangepast aan de geconstateerde risico's en aanvullende maatregelen getroffen.	The grid operator will have linked the risk management process to the incident management process. Resulting insights will be used to update existing measures and implement new ones.
G1.3.0	Beheersmaatregel	Identificatie van meters dient plaats te vinden op basis van meternummer (inclusief KEMA/KIWA code en bouwjaar) of combinatie van een metertype en serienummer.	Identification of meters will be performed using the meter id (including KEMA/KIWA code and year) or the combination of meter type and serial number.
G1.4.0	Beheersmaatregel	In Meters dienen nooit persoonsgegevens, lokatiespecifieke informatie of EAN-codes opgeslagen te zijn, uitgezonderd meetgegevens.	Personal Data, location specific information or EAN-codes shall never be stored in Meters except for metering data.
G1.5.0	Beheersmaatregel	Het dient niet mogelijk te zijn verbruikspatronen af te leiden van de frequentie of omvang van berichtenverkeer vanaf de meter, waaronder het P2 of P3-verkeer.	It must be impossible to deduce consumption patterns using the frequency or intensity of data traffic from the meter, including P2 or P3 traffic.

G1.6.0	Beheersmaatregel	Bij de aanstelling tekenen alle medewerkers die met persoonsgegevens zullen gaan werken een geheimhoudingsverklaring. Dit geldt ook voor tijdelijke medewerkers.	All employees that will be processing personal data will sign a non-disclosure agreement during on-boarding. This also applies to temporary staff.
G2.0.0	Beheersdoelstelling	De netbeheerder beheerst de omgang met verwerkers.	The grid operator controls the Processor.
G2.1.0	Beheersmaatregel	Indien bij de verwerking van Persoonsgegevens gebruik wordt gemaakt van een verwerker, sluit de Netbeheerder een overeenkomst met de verwerker voor de beveiliging van de Persoonsgegevens.	If a Processor is used for processing Personal Data, the grid operator will contractually bind the Processor for the security of Personal Data.
G2.1.1	Implementatierichtlijn	De Netbeheerder kan bij de Verwerking van Persoonsgegevens gebruik maken van een verwerker. In dat geval zal de Netbeheerder met de verwerker een overeenkomst sluiten, waarin schriftelijk of in een andere, gelijkwaardige vorm onder meer de technische en organisatorische maatregelen ter beveiliging van die Persoonsgegevens worden vastgelegd.	The Grid Operator can use a Processor for processing Personal Data. In that case the Grid Operator will enter into a contract (paper or equally binding) with the Processor that covers inter alia the technical and organizational measures to secure that Personal Data.
G2.2.0	Beheersmaatregel	Verantwoordelijkheden en taken van medewerkers binnen de netbeheerder betreffende privacy en informatiebeveiliging dienen te zijn gedefinieerd, vastgelegd en geïmplementeerd.	Responsibilities and tasks of grid operator employees regarding privacy and information security must be defined, recorded and implemented.
G2.3.0	Beheersmaatregel	De Netbeheerder stelt Persoonsgegevens slechts beschikbaar aan medewerkers, inclusief medewerkers van de verwerker, voor zover die de Persoonsgegevens redelijkerwijs nodig hebben voor de uitoefening van hun taken.	The grid operator will provide Personal Data to employees only and so far these data are a reasonable prerequisite to the execution of their tasks.
G2.4.0	Beheersmaatregel	Iedere Netbeheerder draagt er zorg voor dat zijn medewerkers die betrokken zijn bij de Verwerking van de Persoonsgegevens zich bewust zijn van het belang van een zorgvuldige Verwerking van de Persoonsgegevens en de verplichtingen die op de Netbeheerder rusten.	Every grid operator will ensure that employees tasked with processing Personal Data are aware of the need for careful processing and are aware of the obligations that reside with the grid operator.
G2.5.0	Beheersmaatregel	Iedere Netbeheerder dient een medewerker aan te stellen wiens taak het is om namens het management zorg te dragen voor de naleving van de Privacy en Security slimme-meterinfrastructuur en de Gedragscode dan wel daarop toe te zien.	Every grid operator must appoint an official who is tasked on behalf of the board to assure compliance to Privacy and Security advanced metering infrastructure en the Code of Conduct.
G2.5.1	Implementatierichtlijn	Het aanstellen van een verantwoordelijke medewerker, kan door een speciale rol in de organisatie in te richten. Deze rol hoeft niet voltijds te worden ingevuld.	Appointing the responsible official can be performed using a special role. The role does not require to be an entire FTE.
G2.6.0	Beheersmaatregel	Netbeheerders dragen zorg voor het planmatig verkrijgen van zekerheid over de naleving van verwerkersovereenkomsten door bewerkers.	Grid operators are responsible for the systematic acquisition of assurance about the compliance with processing agreements by processors.
G3.0.0	Beheersdoelstelling	De netbeheerders trachten intern en sectorbreed inzicht te krijgen in de mate van beheersing van Privacy en Security.	Grid operators will strive to obtain sector-wide insight in the compliance to Privacy and Security Requirements.

G3.1.0	Beheersmaatregel	De Netbeheerders stellen gezamenlijk een sectorbrede audit in, om te onderzoeken in hoeverre de sectorbrede zelfregulering van de Privacy en Security slimme-meterinfrastructuur en de Gedragscode zijn geimplementeerd.	The Grid Operators will constitute a sector-wide audit to assess to what extent the self-regulation based on the Privacy and Security Requirements advanced metering infrastructure and the Code of Conduct has been implemented.
G3.2.0	Beheersmaatregel	De Netbeheerder stelt een eigen audit in, waarin de sectorbrede zelfregulering van de Privacy en Security slimme-meterinfrastructuur en de Gedragscode een onderdeel van zijn.	Individual Grid Operators will constitute a internal audit to assess to what extent the sector-wide self-regulation based on the Privacy and Security Requirements advanced metering infrastructure and the Code of Conduct has been implemented.
G3.2.1	Implementatierichtlijn	Netbeheer Nederland kan in overleg met haar leden specifieke aandachtspunten voor de audit voorstellen.	In consultation with its members Netbeheer NL can propose specific points of attention for the audit.
G3.3.0	Beheersmaatregel	Iedere Netbeheerder stelt eens per twee jaar een auditplan vast ter controle op de naleving van de sectorbrede zelfregulering van de Privacy en Security slimme-meterinfrastructuur en de Gedragscode.	Every individual Grid Operators will establish a bi-yearly audit plan to evaluate the compliance to the sector-wide self-regulation based on the Privacy and Security Requirements and the Code of Conduct.
G4.0.0	Beheersdoelstelling	De netbeheerder verwerkt Persoonsgegevens slechts conform de doeleinden in de Gedragscode. Daar waar wordt afgeweken, is dit afgedekt middels een hiaatverklaring.	The Grid Operator will process Personal Data only in accordance with the goals stated in the Code of Conduct.
G4.1.0	Beheersmaatregel	De Netbeheerder verwerkt Metergegevens in het kader van het beheer van het elektriciteits- en/of gasnet, de Meter en daarmee samenhangende activiteiten. Tot deze categorie van verwerkingen behoort: - Technisch beheer van het Net.	The Grid Operator shall process Smart Meter Data only for the purposes of managing the electricity and gas grids, the Smart Meter and related activities. Technical management of the grid is a part of these activities.
G4.1.1	Implementatierichtlijn	De Netbeheerder kan Metergegevens verwerken in het kader van het technisch beheer van het Net. Hieronder vallen onder meer de volgende activiteiten: a) Het lokaliseren en oplossen van spanningsonderbrekingen; b) Het uitvoeren van besturingsopdrachten; c) Het verbeteren van de bedrijfsvoering en doelmatig netbeheer; d) Het beperken van netverlies; en e) Het faciliteren van energietransitie.	The Grid Operator can process Smart Meter Data for the purpose of technical management of the grid. Some of the activities performed as a part of this technical management are: a) Locating and solving voltage interruptions b) Executing control orders c) Improving business operations and functional control d) Reducing grid loss e) Facilitating energy transition.
G4.1.2	Implementatierichtlijn	In het kader van het technisch beheer van het Net kan indien nodig via de Meter monitoringinformatie worden verzameld en verwerkt. Deze Metergegevens worden door de Netbeheerder uitsluitend gebruikt voor het monitoren van de netkwaliteit, het lokaliseren van storingen en het uitkeren van vergoedingen bij storingen.	Where necessary, monitoring information may be collected and processed via the Smart Meter for the purpose of technical control of the Grid. The Grid Operator shall only use such Smart Meter Data for the monitoring of power quality, locating interruptions and compensation in case of outages.
G4.1.3	Implementatierichtlijn	Indien de Kleinverbruiker heeft aangegeven dat de Meter administratief uit moet staan, is het niet toegestaan de Meter op afstand uit te lezen voor het technisch beheer van het Net.	Where Smart Meter is switched to ‘remote read out opt-out’ following the Private Consumer’s request in accordance with article 6.1.3.1, it is not allowed to remotely read the Smart Meter for the purposes of technical control of the Grid.

G4.2.0	Beheersmaatregel	De Netbeheerder verwerkt Metergegevens in het kader van het beheer van het elektriciteits- en/of gasnet, de Meter en daarmee samenhangende activiteiten. Tot deze categorie van verwerkingen behoort: - Metrologisch beheer.	The Grid Operator will process Smart Meter Data for the purpose of managing the electricity and/or gas grids, the Smart Meter and related activities. Meter Management is one of these activities.
G4.2.1	Implementatierichtlijn	De Netbeheerder kan Metergegevens verwerken in het kader van het beheer van de Meter ("metrologisch beheer"). Onder metrologisch beheer vallen onder meer de volgende activiteiten: a) Het synchroniseren van de in de Meter ingebouwde klok en kalender; b) Het controleren van de batterijstatus van de Meter; c) Het onderhouden van de Meter, zoals het updaten van de firmware; d) Het detecteren van storingen; e) Het handelen op basis van statusinformatie van de Meter (zoals indicatoren, alarmeringen en foutmeldingen); en f) Het testen van het correct functioneren van de meter.	The Grid Operator may process Smart Meter Data in connection with the management of the Smart Meter. This includes at least the following activities: a) Synchronising the clock and calendar embedded in the Smart Meter b) Checking the battery status of the Smart Meter c) Maintaining the Smart Meter, such as updating the firmware d) Detecting failures e) Acting on the basis of status information of the Smart Meter (such as indicators, alarms and failure notifications) f) Testing the correct functioning of the Smart Meter.
G4.2.2	Implementatierichtlijn	De Metergegevens die in het kader van metrologisch beheer worden verzameld, worden door de Netbeheerder uitsluitend gebruikt voor metrologisch beheer.	The Grid Operator shall use the Smart Meter Data, which have been collected for the purpose of meter management, only for the management of the Smart Meter.
G4.2.3	Implementatierichtlijn	Direct na plaatsing van de Meter of na het oplossen van een storing kunnen, in afwijking van de door de Kleinverbruiker gemaakte keuzes als bedoeld in artikelen 6.1.3 en 6.1.4, gedurende een redelijke en beperkte termijn Intervalstanden worden verzameld en verwerkt voor het controleren van de goede werking van de Meter. De Netbeheerder vernietigt deze Intervalstanden kort nadat de goede werking van de Meter is vastgesteld.	Contrary to the choices made by the Private Consumer as referred to in articles 6.1.3 and 6.1.4, interval readings may be collected and processed during a reasonable and short period after the Smart Meter has been installed or after a failure has been solved in order to check the correct functioning of the Smart Meter. The Grid Operator will delete these smart meter interval readings shortly after the correct functioning of the Meter has been established.
G4.2.4	Implementatierichtlijn	In het kader van het metrologisch beheer kunnen, in afwijking van de door de Kleinverbruiker gemaakte keuzes over de Uitleesbaarheid van de Meter en de Frequentie van het op afstand uitlezen van de Meter, zo vaak als nodig is Metergegevens, anders dan Meetgegevens, worden verzameld of naar de Meter worden verzonden.	Contrary to the choices made by the Private Consumer as referred to in articles 6.1.3 and 6.1.4, Smart Meter Data, other than Meter Readings, may be collected from or transmitted to the Smart Meter as often as necessary for the purpose of meter management.
G4.3.0	Beheersmaatregel	De Netbeheerder verwerkt Metergegevens in het kader van het beheer van het elektriciteits- en/of gasnet, de Meter en daarmee samenhangende activiteiten. Tot deze categorie van verwerkingen behoort: - Verwerking van Metergegevens in het kader van analyses.	The Grid Operator will process Smart Meter Data for the purpose of managing the electricity and/or gas grids, the Smart Meter and related activities. Processing Smart Meter Data for the purpose of analytics and statistics is one of these activities.

G4.3.1	Implementatierichtlijn	De Netbeheerder kan Metergegevens verwerken voor het uitvoeren van analyses, waaronder het opstellen van groepsprofielen. De Netbeheerder treft de nodige voorzieningen om te verzekeren dat de verdere verwerking van de Metergegevens uitsluitend plaats heeft ten behoeve van de doeleinden genoemd in de eerste volzin, waarbij het uitgangspunt is dat Metergegevens, voor zover deze Persoonsgegevens betreffen, worden aangepast tot niet tot personen herleidbare gegevens.	The Grid Operator may process Smart Meter Data for the purpose of analytics and statistics, including the creation of group profiles. The Grid Operator shall take the necessary protection measures to ensure that Smart Meter Data are only processed for the purposes mentioned in the first sentence. In principle, Smart Meter Data, which also qualify as Personal Data, shall be anonymised.
G4.3.2	Implementatierichtlijn	De Netbeheerder kan de Metergegevens ter beschikking stellen voor wetenschappelijk onderzoek. Voor zover dergelijk onderzoek wordt uitgevoerd door een Derde, worden de in artikel 5.2.4.1 bedoelde voorzieningen, voor zover relevant, omschreven in een tussen de Netbeheerder en de Derde te sluiten overeenkomst.	The Grid Operator may make the Smart Meter Data available for scientific research. Where the research is conducted by a Third Party, the measures referred to in article 5.2.4.1, shall be, insofar relevant, described in a contract entered into between the Grid Operator and the Third Party.
G4.3.3	Implementatierichtlijn	Indien de Kleinverbruiker heeft aangegeven dat de Meter administratief uit moet staan, is het niet toegestaan de Meter op afstand uit te lezen voor de analyses.	Where the Private Consumer has indicated that the Smart Meter should be to switch to “remote read out opt-out” in accordance with article 6.1.3.1, it is not allowed to remotely read the Smart Meter for the analytics as referred to in article 5.2.4.1.
G4.4.0	Beheersmaatregel	De Netbeheerder kan Metergegevens verwerken ten behoeve van Marktfacilitering, waaronder begrepen het uitvoeren van de volgende activiteiten: - Het faciliteren van activiteiten van Derden ten behoeve van het stimuleren van energiebesparing; en - Overige Marktfacilitering.	The Grid Operator may process Smart Meter Data for the purpose of Market Facilitation, which includes at least the following activities: a) Facilitating the activities of Third Parties related to energy-saving b) Other Market Facilitation activities.
G4.4.1	Implementatierichtlijn	De verwerking van Metergegevens ten behoeve van Marktfacilitering vindt slechts plaats op verzoek van een Energieleverancier of ODA dan wel op grond van de wettelijke taak van de Netbeheerder.	The processing of Smart Meter Data for the purpose of Market Facilitation is only allowed at the request of an Energy Supplier or ISP, or in connection with the Grid Operator’s statutory duties.
G4.4.2	Implementatierichtlijn	Indien de Kleinverbruiker heeft aangegeven dat de Meter administratief uit moet staan, is het niet toegestaan de Meter op afstand uit te lezen ten behoeve van: - Het faciliteren van activiteiten van Derden ten behoeve van het stimuleren van energiebesparing; en - Overige Marktfacilitering.	Where the Private Consumer has indicated that the Smart Meter should be to switch to “remote read out opt-out” in accordance with article 6.1.3.1, it is not allowed to remotely read the Smart Meter for the purpose of: a) Facilitating the activities of Third Parties related to energy-saving b) Other Market Facilitation activities.
G4.4.3	Implementatierichtlijn	*Stimuleren van energiebesparing door Energieleveranciers en ODA’s.* In het kader van diensten betreffende de besparing of het efficiënter gebruik van energie kan de Netbeheerder Intervalstanden dan wel Meetgegevens ter beschikking stellen aan Energieleveranciers of ODA’s.	*Energy-saving activities of Energy Suppliers and ISP’s.* The Grid Operator may make the Interval Reading or the Meter Readings available to Energy Suppliers and ISP’s in connection with their services related to energy-saving or the more efficient use of energy.

G4.4.4	Implementatierichtlijn	*Stimuleren van energiebesparing door Energieleveranciers en ODA's.* De Netbeheerder stelt 6 keer per jaar de Meetgegevens ter beschikking aan de Energieleverancier ten behoeve van het verbruiksoverzicht, tenzij de Kleinverbruiker overeenkomstig artikel 6.1.3.1 heeft aangegeven dat de Meter administratief uit staat.	*Energy-saving activities of Energy Suppliers and ISP's.* Six (6) times a year, the Grid Operator shall make the Meter Readings available to Energy Suppliers for the purpose of preparation of the consumption statement, unless the Private Consumer, has indicated that the Smart Meter should be switched to "remote read out opt-out" in accordance with article 6.1.3.1.
G4.4.5	Implementatierichtlijn	*Stimuleren van energiebesparing door Energieleveranciers en ODA's.* De doorgifte van Intervalstanden aan een Energieleverancier of een ODA vindt slechts plaats indien de Kleinverbruiker daar vooraf overeenkomstig AVG artikel 6 sub 1a toestemming voor heeft gegeven aan de Verwerkingsverantwoordelijke.	*Energy-saving activities of Energy Suppliers and ISP's.* The transmission of the Interval Readings to the Energy Supplier or ISP is only allowed with the unambiguous prior consent given by the Private Consumer to the Controller in accordance with GPDR article 6.1.a.
G4.4.6	Implementatierichtlijn	*Overige Marktfacilitering.* De Netbeheerder kan Metergegevens verzamelen en verder verwerken in het kader van overige Marktfacilitering. Onder overige Marktfacilitering vallen onder meer de volgende activiteiten: a) Het beschikbaar stellen van de Meetgegevens ten behoeve van de facturering door de Energieleverancier; b) Activiteiten ten behoeve van variabele tarifering; en c) Het versturen van besturingsopdrachten naar de Meter.	*Other Market Facilitation.* The Grid Operator may collect and further process Smart Meter Data for the purpose of other Market Facilitation activities. This includes at least: a) Making the Meter Readings available to the Energy Supplier for the purpose of billing b) Activities in the context of variable pricing c) Sending control commands to the Smart Meter.
G4.4.7	Implementatierichtlijn	*Overige Marktfacilitering.* De Netbeheerder stelt zo vaak als nodig de Meetgegevens ter beschikking aan de Energieleverancier ten behoeve van de facturatie, ten minste jaarlijks en bij wijzigingen bij de Kleinverbruiker, zoals verhuizing, overgang naar een andere Energieleverancier, overgang van Kleinverbruiker naar grootverbruiker, beëindiging van de aansluiting of contractbeëindiging (zoals bij overlijden van de enige Kleinverbruiker op het adres).	*Other Market Facilitation.* The Grid Operator makes the Smart Meter Data available to the Energy Supplier as often as necessary for the purpose of billing, at least once a year and in the case of changes at the side of the Private Consumer, such as change of address, change of Energy Supplier, transition of Private Consumer to a large capacity consumer, or termination of the connection or contract (such as in case of death of the only Private Consumer at an address).
G4.4.8	Implementatierichtlijn	*Overige Marktfacilitering.* De Metergegevens worden door de Netbeheerder slechts verstrekt aan de Energieleverancier waarmee de betreffende Kleinverbruiker een contract heeft betreffende de levering van elektriciteit of gas. Deze Metergegevens worden niet verzameld met een interval korter dan die welke met de Kleinverbruiker is overeengekomen ingevolge artikel 6.1.4.	*Other Market Facilitation.* The Grid Operator shall disclose the Smart Meter Data only to the Energy Supplier, which has a contract with the Private Consumer concerning the supply of electricity or gas. Smart Meter Data shall not be collected with intervals shorter than as agreed with the Private Consumer in accordance with article 6.1.4.

G4.5.0	Beheersmaatregel	Verwerkingen ten behoeve van Overige Activiteiten (aan de Kleinverbruiker) De Netbeheerder kan Metergegevens verzamelen en verwerken ten behoeve het aanbieden van Overige Activiteiten.	The Grid Operator may collect and process Smart Meter Data for the purpose of offering Other Services.
G4.5.1	Implementatierichtlijn	Verwerking van Metergegevens ten behoeve van Overige Activiteiten is slechts toegestaan indien dit noodzakelijk is voor de uitvoering van een overeenkomst voor Overige Activiteiten waarbij de Kleinverbruiker partij is dan wel met diens ondubbelzinnige voorafgaande toestemming.	Processing Smart Meter Data for the purpose of Other Services is only allowed insofar necessary for the performance of a contract for Other Services to which the Private Consumer is party or with his unambiguous prior consent.
G4.5.2	Implementatierichtlijn	Indien ten behoeve van een Overige Activiteit Metergegevens nodig zijn, die door de Netbeheerder zijn verzameld ten behoeve van de uitvoering van de activiteiten voor marktfacilitering, informeert de Netbeheerder de Kleinverbruiker hierover specifiek op het moment dat de toestemming wordt gevraagd voor het verzamelen of gebruik van de Metergegevens ten behoeve van een Overige Activiteit, dan wel bij het aangaan van de overeenkomst voor een Overige Activiteit.	If Smart Meter Data, which have been collected by the Grid Operator for the purpose of activities referred to in article 5.3.1, are needed for Other Services, the Grid Operator shall specifically inform the Private Consumer about such use when requesting consent for the collection and use of Smart Meter Data for the purpose of the Other Service, or at the time the contract for the Other Service is entered into.
G4.5.3	Implementatierichtlijn	Indien de Kleinverbruiker overeenkomstig heeft aangegeven dat de Meter administratief uit moet staan, is het niet toegestaan de Meter op afstand uit te lezen ten behoeve van de Overige Activiteiten.	Where the Private Consumer, in accordance with article 6.1.3.1, has indicated that the Smart Meter should be to switch to “remote read out opt-out”, it is not allowed to remotely read the Smart Meter for the Other Services referred to in article 5.4.1.
G4.6.0	Beheersmaatregel	De netbeheerder mag Persoonsgegevens verwerken voor: - Het uitvoeren van enige andere wettelijke verplichting van de Netbeheerder voor zover deze niet reeds behoort tot: - Het beheer van elektriciteits- en gasnetten, de Meter en daarmee samenhangende activiteiten. - Het faciliteren van diensten van een Energieleverancier of een ODA aan een Kleinverbruiker.	The Grid Operator may process Personal Data for the purposes of complying with any other legal obligation of the Grid Operator insofar this is not already a part of: - Managing the electricity and gas grids, the Smart Meter and related activities - Facilitating the services of an Energy Supplier or ISP to the Private Consumer.
G5.0.0	Beheersdoelstelling	De Netbeheerder verwerkt persoonsgegevens volgens legitieme grondslagen.	The Grid Operator will process Personal Data according to legitimate foundations.

G5.1.0	Beheersmaatregel	De verwerking is alleen rechtmatig indien en voor zover aan ten minste een van de onderstaande voorwaarden is voldaan: a) de betrokkene heeft toestemming gegeven voor de verwerking van zijn persoonsgegevens voor een of meer specifieke doeleinden; b) de verwerking is noodzakelijk voor de uitvoering van een overeenkomst waarbij de betrokkene partij is, of om op verzoek van de betrokkene vóór de sluiting van een overeenkomst maatregelen te nemen; c) de verwerking is noodzakelijk om te voldoen aan een wettelijke verplichting die op de verwerkingsverantwoordelijke rust; d) de verwerking is noodzakelijk om de vitale belangen van de betrokkene of van een andere natuurlijke persoon te beschermen; e) de verwerking is noodzakelijk voor de vervulling van een taak van algemeen belang of van een taak in het kader van de uitoefening van het openbaar gezag dat aan de verwerkingsverantwoordelijke is opgedragen; , f) de verwerking is noodzakelijk voor de behartiging van de gerechtvaardigde belangen van de verwerkingsverantwoordelijke of van een derde, behalve wanneer de belangen of de grondrechten en de fundamentele vrijheden van de betrokkene die tot bescherming van persoonsgegevens nopen, zwaarder wegen dan die belangen, met name wanneer de betrokkene een kind is.	Processing shall be lawful only if and to the extent that at least one of the following applies: a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes; b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; c) processing is necessary for compliance with a legal obligation to which the controller is subject; d) processing is necessary in order to protect the vital interests of the data subject or of another natural person; e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.
G5.1.1	Implementatierichtlijn	Hierbij geldt dat het centraal systeem dient te beschikken over functionaliteit om te monitoren welke data (waaronder intervalstanden) over welke periode bij klanten zijn opgehaald.	For the processing of Personal Data the Central System will provide functionality to monitor which data (including interval readings) have been retrieved from clients during which period.
G5.2.0	Beheersmaatregel	De Netbeheerder verwerkt Persoonsgegevens slechts voor andere doeleinden voor zover een dergelijke verwerking niet onverenigbaar is met de doeleinden waarvoor de Netbeheerder de Persoonsgegevens oorspronkelijk heeft verkregen ("Nevengebruik").	The Grid Operator shall process Personal Data only for other purposes insofar such processing is not incompatible with the purposes for which the Grid Operator has originally obtained the Personal Data (“Further Processing”).
G5.2.1	Implementatierichtlijn	Bij zulks Nevengebruik van de Persoonsgegevens zorgt de Netbeheerder, gelet op de verwantschap tussen het beoogde doel en het doel waarvoor de gegevens oorspronkelijk zijn verkregen, de aard van de Persoonsgegevens, de te verwachten gevolgen van het Nevengebruik voor de Kleinverbruiker en de wijze waarop de gegevens zijn verkregen, voor passende waarborgen voor de bescherming van de persoonlijke levenssfeer van de Kleinverbruiker.	Where the Personal Data are Further Processed, the Grid Operator shall ensure that appropriate safeguards for the protection of the privacy of the Private Consumer are taken in view of the relationship between the envisaged purpose and the purpose for which the data where originally obtained, the nature of the Personal Data, the expected consequences of the Further Processing for the Private Consumer and the way in which the data were obtained.

G5.3.0	Beheersmaatregel	De Netbeheerder neemt maatregelen zodat Persoonsgegevens, gelet op de doeleinden waarvoor zij door de Netbeheerder worden verwerkt, accuraat, toereikend, ter zake dienend en niet bovenmatig zijn.	The Grid Operator shall implement measures to ensure that Personal Data, given the purposes for which the Grid Operator processes the data, are accurate, sufficient, relevant and not excessive.
G5.4.0	Beheersmaatregel	De Netbeheerder bewaart Persoonsgegevens niet langer dan noodzakelijk voor de doeleinden.	The Grid Operator shall not retain Personal Data longer than necessary for the purposes described.
G5.4.1	Implementatierichtlijn	Hierbij geldt dat bewaartermijnen van meterstanden in het centraal systeem zijn gemaximeerd: - voor intervalstanden: 10 kalenderdagen. - voor dagstanden: 24 maanden. - voor maandstanden: 13 maanden	In this context retention periods for metering data are limited: - for interval readings: 10 calendar days - for daily meter readings: 24 months - for monthly meter readings: 13 months.
G5.4.2	Implementatierichtlijn	Hierbij geldt dat ongeacht de capaciteit van apparaten om meterstanden op te slaan de bewaartermijnen van data hardwarematig of via de configuratie zijn gemaximeerd: - voor intervalstanden: 10 kalenderdagen - voor dagstanden: 40 kalenderdagen - voor maandstanden: 13 maanden	The data retention periods will be limited hard wired or configured, regardless the capacity of system assets to store meter readings, as follows: - for interval readings: 10 calendar days - for daily meter readings: 40 calendar days - for monthly meter readings: 13 months.
G5.4.3	Implementatierichtlijn	Na het verlopen van de bewaartermijnen in systeemassets dienen persoonsgegevens te worden verwijderd.	Personal Data in system assets will be removed upon expiration of the retention period.
G5.5.0	Beheersmaatregel	De netbeheerder informeert de kleinverbruiker tijdig en adequaat over het verzamelen van persoonsgegevens.	The Grid Operator shall inform the Private Consumer timely and adequately of the collection of Personal Data.
G5.5.1	Implementatierichtlijn	De eisen wat betreft: - Persoonsgegevens volgens legitieme grondslagen verwerken en het nevengebruik daarvan; - Persoonsgegevens volgens legitieme grondslagen verwerken en de kleinverbruiker daarover juist informeren; en - Rechten van de kleinverbruiker wat betreft de metergegevens (recht van inzage, correctie en verzet); kunnen in bijzondere omstandigheden, waarbij alle feiten en omstandigheden van belang zijn, opzij worden gezet als hiertoe een dringende noodzaak bestaat, voor zover deze noodzaak zwaarder weegt dan de rechten en vrijheden van de Kleinverbruiker.	In exceptional circumstances, provided due consideration is given to all relevant facts and circumstances, the following requirements may be set aside if a pressing need to do so exists, and provided such need outweighs the rights and freedoms of the Private Consumer: - Processing and Further Processing of Personal Data is performed in accordance with legitimate foundations - Personal Data will be processed in accordance with legitimate foundations en the Private Consumer will be informed correctly and adequately of such processing - The Private Consumer has the right of access to and correction of the Smart Meter Data, as well as the right to object to the processing of that data.

G5.5.2	Implementatierichtlijn	Indien Persoonsgegevens worden verzameld bij de Kleinverbruiker, informeert de Netbeheerder de Kleinverbruiker over zijn identiteit en de doeleinden van de Verwerking van Persoonsgegevens. Hiernaast verstrekt de Netbeheerder de Kleinverbruiker informatie voor zover dat gelet op de aard van de gegevens, de omstandigheden waaronder zij worden verkregen of het gebruik dat ervan wordt gemaakt, nodig is om tegenover de Kleinverbruiker een behoorlijke en zorgvuldige verwerking te waarborgen. Indien de Netbeheerder gegevens verzamelt met ondubbelzinnige toestemming, dan informeert de Netbeheerder de Kleinverbruiker tevens over de consequenties die daaraan verbonden zijn en het feit dat deze zijn toestemming te allen tijde weer kan intrekken. Aan deze informatieplicht wordt voldaan vóór het moment dat de Persoonsgegevens via de Meter worden verzameld. De informatie hoeft niet te worden verstrekt indien de Netbeheerder op goede gronden mag aannemen dat de Kleinverbruiker daarvan reeds op de hoogte is of als de gegevens worden verwerkt ten behoeve van een Energieleverancier of een ODA waarmee de Kleinverbruiker een contract heeft gesloten, in welk geval de Netbeheerder mag aannemen dat de Kleinverbruiker al door de Energieleverancier of de ODA is geïnformeerd.	Where Personal Data are collected from the Private Consumer, the Grid Operator shall inform the Private Consumer of his identity and the purposes of the processing of the Personal Data. Furthermore, the Grid Operator shall provide information to ensure a fair processing with respect to the Private Consumer, given the nature of the data, the circumstances in which the data were obtained or the use of the data. Where the Grid Operator collects Personal Data on the basis of the Private Consumer's unambiguous consent as referred to in article 5.4.2, the Grid Operator shall inform the Private Consumer also of the consequences of his consent as well as of the fact that consent may be withdrawn at any time. The obligation to inform the Private Consumer needs to be complied with prior to the collection of Personal Data via the Smart Meter. The information does not need to be provided where the Grid Operator may reasonably assume that the Private Consumer already has such information or where the data are processed on behalf of an Energy Supplier or ISP with which the Private Consumer has entered into a contract. In such case, the Grid Operator may assume that the Private Consumer already has been informed by the Energy Supplier or the ISP.
G5.6.0	Beheersmaatregel	De Netbeheerder zal waar de AVG dit vereist een eigen verwerkingenregister inrichten voor het registreren van de verwerking van persoonsgegevens gerelateerd aan de slimme-meterinfrastructuur.	The Network Manager will set up its own processing register where the AVG requires it to register the processing of personal data related to the smart meter infrastructure.
G5.7.0	Beheersmaatregel	De Netbeheerder zal een bij de AP te registreren Functionaris Gegevensbescherming aanwijzen die toeziet op de verwerking van slimme meter gegevens conform de vereisten van de AVG.	The DSO will assign a Data Protection Officer to be registered with the AP who supervises the processing of smart meter data in accordance with the requirements of the AVG.
G6.0.0	Beheersdoelstelling	De netbeheerder verwerkt Metergegevens en Persoonsgegevens slechts indien de rechten van de Kleinverbruiker worden gerespecteerd.	The Grid Operator shall process Meter Readings and Personal Data only if de rights of the Private Consumer are respected.
G6.1.0	Beheersmaatregel	De netbeheerder informeert de "Kleinverbruiker binnen een redelijke termijn voorafgaande aan de plaatsing van de Meter over de verschillende keuzes betreffende de verwerking van Metergegevens. Deze keuzes betreffen: a) De plaatsing van de Meter; b) De uitleesbaarheid van de Meter; en c) De frequentie van het op afstand uitlezen van de Meter.	Within a reasonable time prior to the installation of the Smart Meter, the Private Consumer must be informed about the various choices with respect to the processing of Smart Meter Data. These choices concern: a) The installation of the Smart Meter b) The remote readability of the Smart Meter c) The frequency with which the Smart Meter is remotely read.

G6.2.0	Beheersmaatregel	De netbeheerder stelt een interne klachtenprocedure in en werkt mee aan de reguliere geschillenbeslechting bij de Geschillencommissie Energie en Water.	The Grid Operator shall implement an internal dispute resolution procedure and will cooperate with regular dispute resolution by the Arbitration Board for Energy and Water.
G6.2.1	Implementatierichtlijn	De Netbeheerder maakt het mogelijk dat de Kleinverbruiker een interne klachtenprocedure kan doorlopen. Dit is namelijk een voorwaarde die eerst vervult moet worden, voor geschillenbeslechting bij de Geschillencommissie Energie en Water. Na deze interne klachtenprocedure bij Netbeheerder kan de Kleinverbruiker zich wenden tot de Geschillencommissie Energie en Water. De Netbeheerder werkt mee aan de reguliere geschillenbeslechting bij de Geschillencommissie Energie en Water.	The Grid Operator will enable Private Consumers to enter an internal dispute resolution procedure. Completing this procedure is a prerequisite for dispute resolution by the Arbitration Board for Energy and Water. Only after entering the internal dispute resolution procedure with the Grid Operator can the Private Consumer apply to the Arbitration Board for Energy and Water. The Grid Operator will cooperate with regular dispute resolution by the Arbitration Board for Energy and Water.
G6.2.2	Implementatierichtlijn	Elke Netbeheerder houdt een overzicht bij van de geschillen en hun uitkomsten.	Grid operators are required to keep an overview of all disputes and their outcome.
G6.3.0	Beheersmaatregel	De netbeheerder plaatst geen Slimme Meter bij de kleinverbruiker, indien "de Kleinverbruiker voorafgaand aan de plaatsing van de Meter aan de Netbeheerder te kennen heeft gegeven bezwaar te hebben tegen de plaatsing van de Meter, wordt geen Meter geplaatst." Daarbij geldt wel dat een "Meter die reeds geplaatst is, kan niet meer op verzoek van de Kleinverbruiker worden vervangen door een niet op afstand uitleesbare meter."	The Grid Operator will not install a Smart Meter at the Private Consumer if the Private Consumer has communicated his objection to the installation of such a Meter prior to the installation event. Note that if a Smart Meter has already been installed, it cannot be replaced by a Traditional Meter without remote access capabilities.
G6.3.1	Implementatierichtlijn	De netbeheerders stelt periodiek vast of de weigering van de kleinverbruiker juist is geregistreerd.	The Grid Operator will assess periodically whether Private Consumer objections have been registered accurately.
G6.4.0	Beheersmaatregel	De Kleinverbruiker kan de Netbeheerder te allen tijde verzoeken om de uitleesbaarheid van een Slimme Meter op afstand te wijzigen.	The Private Consumer has the right to request the grid Operator to change the remote reading settings of the Meter.
G6.4.1	Implementatierichtlijn	De netbeheerder zorgt ervoor dat uitleesbaarheid op afstand van een Slimme Meter kan worden aangezet (“administratief aan”) of worden uitgezet (“administratief uit”). De Netbeheerder voert dit verzoek zo spoedig mogelijk uit.	The Grid Operator ensures that the remote reading settings of a Meter can be switched on (administratively up) or switched off (administratively down). The Grid Operator will execute such a request as soon as possible.
G6.4.2	Implementatierichtlijn	De netbeheerders stelt periodiek vast of het verzoek van administratief uit van de kleinverbruiker juist is geregistreerd.	The Grid Operator shall assess periodically whether the opt-out requests by Private Consumers have been registered accurately.
G6.5.0	Beheersmaatregel	De netbeheerder houdt zich aan de toegestane frequentie van het op afstand uitlezen van de Slimme Meter.	The Grid Operator shall comply to the allowed frequency of remote readings of the Meter.

G6.5.1	Implementatierichtlijn	"Indien een Kleinverbruiker geen keuze betreffende de frequentie van het op afstand uitlezen kenbaar maakt, wordt de Slimme Meter door de Netbeheerder als volgt op afstand uitgelezen: a) Eén keer per jaar ten behoeve van het opmaken van de jaarnota door de Energieleverancier; b) Tweemaandelijks ten behoeve van het inzicht in het energieverbruik; en c) Incidenteel voor zover noodzakelijk voor een wisseling van Energieleverancier, verhuizing of opzegging van de aansluiting, technisch beheer van het Net of het metrologisch beheer." "Het uitlezen van de Slimme Meter met een hogere frequentie dan de genoemde standaard behoeft de ondubbelzinnige voorafgaande toestemming van de Kleinverbruiker aan de Energieleverancier of ODA dan wel een overeenkomst tussen de Kleinverbruiker enerzijds en de Energieleverancier of de ODA anderzijds." Daarbij kan de "Kleinverbruiker te allen tijde de toestemming via de Energieleverancier of ODA intrekken."	Where the Private Consumer has not made a choice with regard to the frequency, with which the Smart Meter may be remotely read, the Grid Operator shall remotely read the Smart Meter in accordance with the following schedule: (a) Once per year for the purpose of preparing the bill by the Energy Supplier; (b) Once every two (2) months for the purpose of awareness about the energy consumption; (c) Ad hoc insofar necessary for the change of Energy Supplier, change of address, termination of the connection, technical control of the Grid, or management of the Smart Meter. Reading the Smart Meter with a higher frequency requires the unambiguous prior consent of the Private Consumer given to the Energy Supplier or ISP, or a contract between the Private Consumer and the Energy Supplier or ISP. The Private Consumer has the right to withdraw his consent at any time via the Energy Supplier or ISP.
G6.6.0	Beheersmaatregel	Onverminderd het bepaalde in en krachtens de Elektriciteitswet 1998, de Gaswet en de Algemene Voorwaarden heeft een Kleinverbruiker het recht van inzage en correctie van de Metergegevens, alsmede het recht van verzet tegen de verwerking van Metergegevens door de Netbeheerder.	Without prejudice to the Electricity Act of 1998, the Gas Act and the Terms & Conditions and articles 4.12 to 4.15 of this Code, the Private Consumer has the right of access to and correction of the Smart Meter Data, as well as the right to object to the processing of Smart Meter Data by the Grid Operator.
G6.6.1	Implementatierichtlijn	Voor de uitoefening van dit bovenstaande rechten dient de Kleinverbruiker zich te wenden tot de Netbeheerder waarmee hij of zij een overeenkomst heeft betreffende de aansluiting op het elektriciteits- of gasnet of het transporteren van elektriciteit of gas.	With respect to the exercise of the rights above the Private Consumer should address the Grid Operator with which he has a contract related to the connection to the electricity or gas grid or the transport of electricity or gas.
G6.6.2	Implementatierichtlijn	De Netbeheerder kan een verzoek van de Kleinverbruiker om correctie van de Persoons- of Metergegevens afwijzen, indien de Kleinverbruiker de bepalingen in de Algemene Voorwaarden die relevant zijn voor de juiste vaststelling van de Meetgegevens en geschilbeslechting niet in acht heeft genomen.	The Grid Operator may deny a Private Consumer's request for correction of the Personal Data or the Smart Meter Data, as referred to in article 4.13 and 6.2.1, if the Private Consumer did not comply with the terms of the Terms & Conditions related to the correct determination of the Metering Data and dispute resolution.
G6.7.0	Beheersmaatregel	De Netbeheerder geeft, als de Kleinverbuiker daar schriftelijk om vraagt, een overzicht van de hem of haar betreffende persoonsgegevens die worden verwerkt door de netbeheerder.	Upon reception of a written request by the Private Consumer the Grid Operator will provide a written overview of the Personal Data which are processed by the Grid Operator.

G6.7.1	Implementatierichtlijn	De Netbeheerder voldoet aan het recht van de Kleinverbruiker - met redelijke tussenpozen - om schriftelijk een overzicht te vragen van specifieke, hem of haar betreffende Persoonsgegevens die door die Netbeheerder worden Verwerkt. De Netbeheerder zal, behoudens de uitzonderingsgevallen (genoemd in de beheersmaatregel Netbeheerders mogen de beheersmaatregelen over privacy overtreden als hogere doelen daartoe noodzaken), de Kleinverbruiker binnen vier (4) weken na ontvangst van het verzoek een volledig overzicht van de Persoonsgegevens doen toekomen. Ook indien blijkt dat door de Netbeheerder geen Persoonsgegevens van de Kleinverbruiker worden verwerkt, zal de Netbeheerder binnen vier (4) weken na ontvangst van het verzoek de Kleinverbruiker hierover informeren. Het overzicht omvat in begrijpelijke vorm: a) een omschrijving van het doel of de doeleinden van de Verwerking; b) de categorieën van Persoonsgegevens waarop de Verwerking betrekking heeft; c) de ontvangers of categorieën van ontvangers van de Persoonsgegevens, alsmede; en d) de beschikbare informatie over de herkomst van de Persoonsgegevens. De Netbeheerder draagt zorg voor een deugdelijke vaststelling van de identiteit van de verzoeker. De Netbeheerder kan hiervoor een vergoeding van kosten verlangen die niet hoger is dan het bij Besluit Kostenvergoeding Rechten Betrokkenen vastgestelde bedrag. Indien tot aanpassing, wijziging of verwijdering van de gegevens wordt overgegaan of indien het verzet gegrond wordt bevonden wordt het bedrag gerestitueerd.	The Grid Operator will comply to the right of the Private Consumer to ask with reasonable intervals for an overview of specific Personal Data related to him, which are processed by the Grid Operator (‘right of access’). With the exception of cases referred to in article 4.11, the Grid Operator shall provide the Private Consumer with a full overview of the Personal Data within four (4) weeks after receipt of the request. Furthermore, where the Grid Operator does not process Personal Data related to the Private Consumer, the Grid Operator shall inform the Private Consumer within four (4) weeks of this fact. The overview contains in intelligible form: a) the description of the purpose or purposes for which the Personal Data are processed; b) the categories of Personal Data to which the processing relates; c) the recipients or categories of recipients of the Personal Data, and d) the available information as to the origin of the Personal Data. The Grid Operator shall ensure the adequate identification of the person making the request. The Grid Operator may charge compensation for a request of the Private Consumer. Such compensation shall not exceed the maximum sum allowed by the Royal Decree Compensation Execution of Rights Data Subjects (Besluit Kostenvergoeding Rechten Betrokkenen). Where the Personal Data have been corrected, altered or erased or where the objection is valid, the sum shall be refunded.
G6.8.0	Beheersmaatregel	De Netbeheerder voldoet aan het recht van de Kleinverbruiker van correctie van de Metergegevens.	The Grid Operator will comply to the right of the Private Consumer to correction of the Smart Meter Data.
G6.8.1	Implementatierichtlijn	De Netbeheerder voldoet aan het recht van de Kleinverbruiker van correctie van de Metergegevens. (Onverminderd het bepaalde in en krachtens de Elektriciteitswet 1998, de Gaswet en de Algemene Voorwaarden, en de artikelen 4.12 tot en met 4.15 zijn van overeenkomstige toepassing.) De Netbeheerder kan een verzoek van de Kleinverbruiker om correctie van de Persoons- of Metergegevens afwijzen, indien de Kleinverbruiker de bepalingen in de Algemene Voorwaarden die relevant zijn voor de juiste vaststelling van de Meetgegevens en geschilbeslechting niet in acht heeft genomen.	The Grid Operator will comply to the right of the Private Consumer to correction of the Smart Meter Data. (Without prejudice to the Electricity Act of 1998, the Gas Act and the Terms & Conditions and in compliance with articles 4.12 to 4.15 of the Code of Conduct). The Grid Operator may deny a Private Consumer’s request for correction of the Personal Data or the Smart Meter Data if the Private Consumer did not comply with the terms of the Terms & Conditions related to the correct determination of the Metering Data and dispute resolution.

G6.9.0	Beheersmaatregel	De Netbeheerder voldoet aan het recht van de Kleinverbruiker van verbetering, aanvulling, verwijdering of afscherming van zijn of haar persoonsgegevens, indien blijkt (na inzage) dat deze Persoonsgegevens feitelijk onjuist zijn, voor het doel van de verwerking onvolledig of niet ter zake dienend dan wel anderszins in strijd.	The Grid Operator shall comply to the right of the Private Consumer to request correction, completion, erasure or blocking of the Personal Data related to him if the overview referred to in article 4.12 indicates that the Personal Data are factually incorrect, incomplete or irrelevant as to the purposes or otherwise infringes this Code.
G6.9.1	Implementatierichtlijn	De Netbeheerders maakt het mogelijk dat de Kleinverbruiker schriftelijk kan verzoeken om verbetering, aanvulling, verwijdering of afscherming van de betreffende gegevens, indien na inzage van de Persoonsgegevens blijkt dat deze Persoonsgegevens feitelijk onjuist zijn, voor het doel van de verwerking onvolledig of niet ter zake dienend dan wel anderszins in strijd met de Gedragscode worden verwerkt. De Netbeheerder zal de Kleinverbruiker binnen vier (4) weken na ontvangst van genoemd verzoek, schriftelijk laten weten of, dan wel in hoeverre aan het verzoek wordt voldaan. Indien niet of niet volledig aan het verzoek van de Kleinverbruiker wordt voldaan, zal dit met redenen worden omkleed. De Netbeheerder kan hiervoor een vergoeding van kosten verlangen die niet hoger is dan het bij Besluit Kostenvergoeding Rechten Betrokkenen vastgestelde bedrag. Indien tot aanpassing, wijziging of verwijdering van de gegevens wordt overgegaan of indien het verzet gegrond wordt bevonden wordt het bedrag gerestitueerd.	The Grid Operator shall comply to the right of the Private Consumer to request correction, completion, erasure or blocking of the Personal Data related to him if the overview referred to in article 4.12 indicates that the Personal Data are factually incorrect, incomplete or irrelevant as to the purposes or otherwise infringes this Code. The Grid Operator shall inform the Private Consumer in writing within four (4) weeks after receipt of the request whether and, if so, to what extent the request has been complied with. Where a request of the Private Consumer is not or not entirely complied with, the Grid Operator shall explain the reasons for the refusal. The Grid Operator may charge compensation for a request of the Private Consumer . Such compensation shall not exceed the maximum sum allowed by the Royal Decree Compensation Execution of Rights Data Subjects (Besluit Kostenvergoeding Rechten Betrokkenen). Where the Personal Data have been corrected, altered or erased or where the objection is valid, the sum shall be refunded.
G6.10.0	Beheersmaatregel	De Netbeheerder voldoet aan het recht van de Kleinverbruiker van verzet tegen de verwerking van Persoonsgegevens door de Netbeheerder.	The Grid Operator will comply to the right of the Private Consumer to object to the processing of Smart Meter Data by the Grid Operator.

G6.10.1	Implementatierichtlijn	De Netbeheerder voldoet aan het recht van de kleinverbuikers om verzet aan te tekenen tegen de Verwerking van Persoonsgegevens in verband met zijn bijzondere persoonlijke omstandigheden, indien de Verwerking van Persoonsgegevens plaatsvindt indien noodzakelijk voor de goede vervulling van de publiekrechtelijke taak van een bestuursorgaan waaraan de Persoonsgegevens worden verstrekt of Netbeheerder verwerkt Persoonsgegevens, indien noodzakelijk voor de behartiging van het gerechtvaardigde belang van de Netbeheerder of van een Derde aan wie de Persoonsgegevens worden verstrekt. Binnen vier (4) weken beoordeelt de Netbeheerder of het verzet gerechtvaardigd is. Is dat het geval dan wordt de Verwerking van Persoonsgegevens van die Kleinverbruiker terstond beëindigd. De Netbeheerder kan hiervoor een vergoeding van kosten verlangen die niet hoger is dan het bij Besluit Kostenvergoeding Rechten Betrokkenen vastgestelde bedrag. Indien tot aanpassing, wijziging of verwijdering van de gegevens wordt overgegaan of indien het verzet gegrond wordt bevonden wordt het bedrag gerestitueerd.	The Grid Operator shall comply to the right of the Private Consumer to object to the processing of his Personal Data in connection with his particular circumstances, unless the Processing of Personal Data is based on one of the following grounds: - the processing is necessary for the proper performance of a public interest task carried out by an administrative body to whom the data are disclosed; or - the processing is necessary for the purposes of the legitimate interests pursued by the Grid Operator or by a Third Party to whom the data are disclosed. The Grid Operator shall review the legitimacy of the objection within four (4) weeks. Where such is the case, the processing of the Personal Data of the Private Consumer shall be terminated immediately. The Grid Operator may charge compensation for a request of the Private Consumer . Such compensation shall not exceed the maximum sum allowed by the Royal Decree Compensation Execution of Rights Data Subjects (Besluit Kostenvergoeding Rechten Betrokkenen). Where the Personal Data have been corrected, altered or erased or where the objection is valid, the sum shall be refunded.
M1.0.0	Beheerdoelstelling *Enkele netbeheerders maken voor het uitlezen en beheren van de slimme meters gebruik van het CTS van een andere netbeheerder. Beheersingsdoelstelling M1.0.0 is toegevoegd om in deze gevallen de naleving van de sectoreisen te toetsen die zijn uitbesteed aan de andere netbeheerder.*	De netbeheerder ziet toe op naleving van de sectoreisen bij uitbesteding van het CTS.	
M1.1.0	Beheersmaatregel	Bij uitbesteding van het CTS stelt de netbeheerder door middel van een onafhankelijk assuranceonderzoek vast of aan de sectoreisen met betrekking tot het CTS wordt voldaan. De netbeheerder neemt kennis van het oordeel van de auditor en neemt waar nodig corrigerende maatregelen in samenspraak met de netbeheerder die het CTS beheert.	

M2.0.0	Beheerdoelstelling *Vanuit de pilots en kleinschalige uitrol voorafgaand aan de grootschalige uitrol van de slimme meter, hebben verschillende netbeheerders nog (beperkte) aantallen 'pre-NTA' meters in het veld hangen. Deze meters vallen buiten de scope van de Privacy- en Security-sectoreisen 2.0 en voldoen dan ook niet op alle gebieden aan deze versie van de sectoreisen. Beheersingsdoelstelling M2.0.0 is toegevoegd om de beheersing van de risico's inzake pre-NTA meters te toetsen.*	De netbeheerder beheerst risico's ten aanzien van slimme meters van de pre-NTA generaties.	
M2.1.0	Beheersmaatregel	De netbeheerder stelt jaarlijks door middel van een dreigingsanalyse vast of ten aanzien van pre-NTA meters aanvullende mitigerende maatregelen benodigd zijn, zoals voortijdige sanering of ontkoppeling van het CTS.	