Alliander Privacy beleid

Integrale aanpak voor optimale beheersing van Privacy risico's

Versie	1.0
Datum	19 juli 2021
Opdrachtgever	Walter Bien (CFO)
Status	Concept
Kerngroep	CPO/FG: Wendy Wieleman Privacy Officers: Jasmijn Ogink, Afshin Ibrahim, Michiel Stoetzer, Loes Derks – van de Ven Privacy Jurist: Jessica van Kraaij
Classificatie	Intern

>	Versielog	Datum	Auteur	Opmerking
	0.6	april	Wendy Wieleman	Eerste versie
	0.8	juni	Wendy Wieleman	Input verwerkt Privacy Officers Input verwerkt Privacy Jurist Input verwerkt CISO Office Input verwerkt Data Office
	0.9	juni	Wendy Wieleman	Externe check input verwerkt Input Liliane Naalden – de Jager en Marc Heideman verwerkt
	1.0	juli	Wendy Wieleman	Finale versie

INHOUD

1 Inleiding

1.1 Doel van dit document

Het doel van dit beleid is om op eenduidige wijze de uitgangspunten op het gebied van privacy te communiceren. Alliander, middels dochteronderneming Liander, heeft de wettelijke taak het gas- en elektriciteitsnet te beheren en te ontwikkelen voor 3,3 miljoen consumenten. Daarnaast zijn binnen Alliander entiteiten als marktpartij actief met producten en diensten die bijdragen aan een toekomstbestendig energienet. Voor een deel van deze (wettelijke) taken is het noodzakelijk om Persoonsgegevens te verwerken. Dit is bijvoorbeeld het geval bij het uitlezen van de slimme meter of het verhelpen van storingen. Daarnaast verwerkt Alliander Persoonsgegevens voor haar interne bedrijfsvoering. Om ervoor te zorgen dat Verwerkingen van Persoonsgegevens in overeenstemming zijn met de toepasselijke wet- en regelgeving, heeft Alliander een aantal maatregelen genomen. Gelet op de aard en hoeveelheid van de Persoonsgegevens die Alliander verwerkt, alsmede gelet op de Algemene Verordening Gegevensbescherming (hierna: AVG), acht Alliander zich gehouden deze maatregelen vast te leggen in dit Alliander Privacy Beleid

Dit document beschrijft het Alliander Privacy Beleid voor de inrichting, implementatie, uitvoering, beheer, monitoring en continue verbetering van Privacy binnen Alliander en haar dochterondernemingen. Het Alliander Privacy beleid dient door de Raad van Bestuur goedgekeurd te zijn. Het Alliander Privacy Beleid wordt jaarlijks beoordeeld op actualiteit, juistheid en volledigheid en waar nodig bijgesteld. Als interne of externe wijzigingen het noodzakelijk maken om het Alliander Privacy Beleid te wijzigen, kunnen tussentijdse aanpassingen plaatsvinden via hernieuwde vaststelling en publicatie.

1.2 Relatie met andere documenten

Dit Alliander Privacy Beleid is een beleidsmatige uitwerking van met name de Algemene Verordening Gegevensbescherming en de Uitvoeringswet Algemene Verordening Gegevensbescherming, op basis van de Privacy Baseline[1] en elementen uit de ISO 27701 norm voor privacy management. Dit Alliander Privacy Beleid is of wordt op zijn beurt uitgewerkt in operationele standaarden en procedures ter invulling van de benodigde beheersmaatregelen.

1.3 Definities

In het Alliander Privacy Beleid worden de volgende definities gehanteerd:

Algemene Verordening Gegevensbescherming (AVG)
Algemene Verordening Gegevensbescherming (EU 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens).

Betrokkene
De persoon op wie de Persoonsgegevens betrekking hebben. De Betrokkene is degene van wie de Persoonsgegevens worden verwerkt.

Datalek
We spreken van een datalek wanneer er sprake is van beveiligingsincident in verband met de beschikbaarheid, integriteit en vertrouwelijkheid van persoonsgegevens, dat per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van

[1] Centrum informatiebeveiliging en Privacybescherming. Grip op Privacy de Privacy Baseline https://www.cip-overheid.nl/media/1554/20201027_Privacybaseline3_3.pdf

of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens (zie artikel 4 onder 12 AVG)[2]

Data Protection Impact Assessment (DPIA)
Dit is een instrument om vooraf de privacyrisico's van een gegevensverwerking in kaart te brengen en vervolgens maatregelen te kunnen nemen om de risico's te verkleinen. Een DPIA is een beoordeling over het effect van de (nieuwe of aangepaste) Verwerking op de bescherming van de Persoonsgegevens en is verplicht als een gegevensverwerking waarschijnlijk een hoog privacyrisico oplevert voor de Betrokkenen. De beoordeling bevat tenminste een inschatting van de risico's van de Verwerking en de vereiste beheersmaatregelen om tekortkomingen op te lossen.

Functionaris Gegevensbescherming (FG)
Een onafhankelijke en deskundige interne toezichthouder en adviseur met wettelijke taken en bevoegdheden. De FG houdt binnen de organisatie toezicht op de toepassing en naleving van alle privacy wet- en regelgeving waaronder de Algemene Verordening Gegevensbescherming (AVG).

Persoonsgegevens
Alle informatie over een identificeerbare of geïdentificeerde natuurlijke persoon. Het gaat hierbij om ieder gegeven dat direct gaat over een persoons ofwel te herleiden is tot een bepaalde persoon (bijvoorbeeld: naam, adres, geboortedatum). Naast "gewone" Persoonsgegevens kent de wet ook bijzondere Persoonsgegevens. Dit zijn gegevens die gaan over gevoelige onderwerpen, zoals etnische achtergrond, politieke voorkeuren of gezondheid.

Verwerker
De organisatie, of persoon, die in opdracht en ten behoeve van de Verwerkingsverantwoordelijke bepaalde onderdelen van of de gehele Verwerking voor zijn rekening neemt.

Verwerkersovereenkomst
Een overeenkomst waarin de afspraken staan hoe een Verwerker met de Persoonsgegevens moet omgaan bij Verwerkingen in opdracht en ten behoeve van de Verwerkingsverantwoordelijke.

Verwerking
Een Verwerking is alles wat je met een Persoonsgegeven doet, zoals: vastleggen, bewaren, verzamelen, bij elkaar voegen, verstrekken aan een ander, en vernietigen.

Verwerkingsverantwoordelijke
De organisatie, of persoon, die bepaalt waarom de Verwerking van Persoonsgegevens plaatsvindt en vaststelt met welke middelen dat gebeurt.

Uitvoeringswet Algemene Verordening Gegevensbescherming (UAVG)
Wet van 16 mei 2018, houdende regels ter uitvoering van Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming) (Pb EU 2016, L 119).

[2] Procedure_Melden_Datalek_Alliander.v.1.0

2 Strategisch kader en uitgangspunten

In deze paragraaf worden de algemeen geldende strategische uitgangspunten beschreven die van toepassing zijn op het Privacy gebied en gelden voor de gehele Alliander organisatie.

2.1 Privacy Missie

Als professionele en betrouwbare netbeheerder hecht Alliander grote waarde aan het vertrouwen van haar klanten, medewerkers en de maatschappij. De Raad van Bestuur draagt daarom, in lijn met de Privacy belangen van klanten, medewerkers en andere betrokkenen, zorg voor een adequate bescherming van persoonsgegevens.

Alliander heeft de afgelopen jaren aandacht en inzet gestopt in het voldoen aan privacy wet- en regelgeving. Gestreefd wordt om te groeien in privacy volwassenheidsniveau. Om dit te bereiken kiest Alliander voor het uiteenzetten van haar ambitie en de uitwerking daarvan in dit Alliander Privacy Beleid. Op basis hiervan zal binnen Alliander gewerkt dienen te worden aan het inbedden van een privacy compliance risicobeheersingsraamwerk dat doorlopend gemonitord wordt. Daarnaast zal er door Alliander structureel geïnvesteerd worden in het vergroten van de bewustwording rondom privacy thema's en het verminderen of voorkomen van privacy risico's.

2.2 Strategisch Kader

Alliander staat voor een energievoorziening die iedereen onder gelijke condities toegang geeft tot betrouwbare, betaalbare en duurzame energie. Dat is waar wij iedere dag aan werken. Het is onze taak om ervoor te zorgen dat het licht brandt, de huizen warm zijn en bedrijven draaien. Zowel vandaag, als in het duurzame morgen. Hierbij hebben de bescherming van de persoonsgegevens van onze klanten en medewerkers en andere betrokkenen, alsmede het imago van Alliander als betrouwbare dienstverlener, continue de aandacht.

- Uitgangspunt is dat persoonsgegevens door Alliander worden verwerkt op een wijze die ten aanzien van de betrokkene rechtmatig, behoorlijk, ethisch en transparant is.

2.3 Werkingssfeer

Het Alliander Privacy Beleid geldt voor de hele organisatie van Alliander N.V. en haar dochterondernemingen. Waar in dit document gerefereerd wordt aan Alliander wordt de scope zoals hierboven genoemd bedoeld.

Het gestelde kader heeft betrekking op alle persoonsgegevens waarvoor Alliander de verwerkingsverantwoordelijkheid heeft of waarvan zij verwerker is. Zoals persoonsgegevens van Alliander medewerkers, alle Alliander processen, alle IT-infrastructuur, alle assets en gebouwen waarin deze zaken zich bevinden en alle relevante leveranciersrelaties waarbij uitwisseling van persoonsgegevens een onderdeel zijn.

2.4 Wettelijk Kader

De AP houdt actief toezicht op de naleving van de AVG en UAVG en kan bij overtreding handhavend optreden richting Alliander en zo nodig maatregelen of sancties opleggen.

Voor Liander als netbeheerder gelden naast de AVG, op grond van de E- en G-wet nog een bevoordelingsverbod, een geheimhoudingsplicht en een gebod om non-discriminatoir te handelen.

2.5 Business Doelstellingen voor Privacy

Naast het ondersteunen van de strategische doelen, streeft Alliander met een adequate inrichting van Privacy tevens de volgende business doelen na:

2.6 Beheer van Risico's

Het privacy control framework van Alliander is vormgegeven door de Privacy Baseline[3] en het Privacy Volwassenheidsmodel van het Centrum Informatiebeveiliging en Privacybescherming (CIP)[4]. Dit dient als het beoordelingskader voor het waarborgen van privacy compliance binnen Alliander. De Privacy Baseline en het Privacy Volwassenheidsmodel van het CIP geven invulling aan het normenkader voor het duiden van compliance risico's en de daarbij behorende beheersmaatregelen binnen Alliander. Op basis van de Privacy Baseline en het Privacy Volwassenheidsmodel zal Alliander kerncontrolepunten en bijbehorende werkprogramma's vaststellen.

De Raad van Bestuur beheert de risico's die een substantiële impact op de strategische doelen of op de bedrijfsvoering van de Alliander organisatie kunnen hebben. Risico's op het gebied van Privacy zijn hier een onderdeel van. De Raad van Bestuur is alert op deze risico's en draagt er zorg voor dat de Alliander organisatie maatregelen treft ter voorkoming van, onder meer, onrechtmatige verwerkingen, Datalekken, en adequaat reageert op onverhoopte incidenten en tekortkomingen om eventuele schade te beperken. Daarnaast hebben het lijnmanagement, de proces-eigenaren, de Functionaris Gegevensbescherming (FG), de Corporate Privacy Officer (CPO), de Privacy jurist en de Privacy Officers een (pro-)actieve rol in het privacy management proces. Deze rollen zijn verder uitgewerkt in sectie 4 van dit document.

2.7 Uitwerking en evaluatie

Dit Alliander Privacy Beleid is ontwikkeld door een cyclisch proces van voorbereiding, ontwikkeling, goedkeuring en evaluatie (Plan-Do-Check-Act). Privacy en gegevensbescherming kunnen door hun dynamiek en toenemend belang op deze wijze effectief worden geborgd. Dit Alliander Privacy Beleid dient door het lijnmanagement uitgewerkt te worden in specifiek uitvoeringsbeleid, nadere richtlijnen en/of werkinstructies. Eén keer per jaar, of eerder indien daar aanleiding toe is, wordt dit Alliander Privacy Beleid geëvalueerd en indien nodig aangepast. Specifiek uitvoeringsbeleid, richtlijnen en werkinstructies zoals het privacy- of het cookie statements, worden eveneens minimaal jaarlijks door het verantwoordelijke lijnmanagement geëvalueerd. De FG schrijft halfjaarlijkse rapportages voor de Raad van Bestuur op basis van het geschreven toezichtplan. Deze rapportages richten zich op specifieke aandachtspunten en het algemene volwassenheidsniveau van Alliander.

[3] https://www.cip-overheid.nl/media/1302/20190506-privacy-baseline-v3_2.pdf

[4] https://www.cip-overheid.nl/media/1141/20171102-privacy-volwassenheidsmodel-v3_0_9.pdf

3 Privacy Beleid

3.1 Privacy Management

3.1.1 Privacy Beleid

Doelstelling: Alliander stelt een Privacy beleid vast waarin is vastgesteld op welke wijze persoonsgegevens worden verwerkt en hoe er invulling wordt gegeven aan de wettelijke beginselen.

De leden van de Raad van Bestuur van Alliander zijn zich bewust van de impact van geldende wet- en regelgeving op het gebied van Privacy en hebben dit Alliander Privacy Beleid vastgesteld om binnen Alliander invulling te geven aan de Privacy principes en eisen van de AVG en de Uitvoeringswet AVG (UAVG) en andere van toepassing zijnde wet- en regelgeving

Uitgangspunt van dit beleid is dat persoonsgegevens door Alliander worden verwerkt op een wijze die ten aanzien van de betrokkene rechtmatig, behoorlijk, ethisch en transparant is.

De Raad van Bestuur is als eigenaar verantwoordelijk voor de bescherming van persoonsgegevens en daarmee ook eigenaar van het Alliander Privacy Beleid. Het Alliander Privacy Beleid wordt beheerd door de Corporate Privacy Officer en wordt gewijzigd wanneer daar aanleiding toe is, op basis van wijzigingen in de strategie of de strategische risico's van Alliander of door externe ontwikkelingen, vanuit bijvoorbeeld veranderende wet- en regelgeving of de rechtspraak.

Het Alliander Privacy Beleid wordt ter goedkeuring voorgelegd aan het Alliander Resilience Committee, en daarna door de Raad van Bestuur wordt vastgesteld.

3.1.2 Afbakening van rollen en verantwoordelijkheden en bijbehorende rapportagelijnen

Doelstelling: Alliander heeft duidelijke rollen en verantwoordelijkheden en bijbehorende rapportagelijnen met betrekking tot de bescherming van persoonsgegevens en het behalen van Privacy doelstellingen belegd, Alliander implementeert deze rollen en verantwoordelijkheden en bijbehorende rapportagelijnen binnen haar organisatie.

De benodigde rollen en verantwoordelijkheden zijn nader beschreven in sectie 4 Governance van dit document. Dit betreft de volgende rollen:

- Raad van Bestuur
- Lijnmanagement
- Corporate Privacy Officer (CPO)
- Medewerkers
- Privacy Officer
- Privacy Jurist
- Corporate Information Security Officer (CISO)
- Functionaris Gegevensbescherming (FG)
- Internal Audit (3de lijns) en External Audit (4de lijns)
- Ondernemingsraad

3.1.3 Privacy Management Systeem

Doelstelling: Alliander beheert de implementatie van dit Privacy beleid en de beheersing van de Privacy risico's vanuit een Privacy managementsysteem dat is gericht op besturing,

aantoonbaarheid en continue verbetering, teneinde invulling te geven aan de eisen vanuit de (U)AVG.

Jaarlijks stelt de CPO samen met de Privacy Officers een jaarplan op waarin de benodigde privacyaspecten en prioriteiten worden geadresseerd. Bij het opstellen van dit jaarplan worden de input vanuit het integrale privacy risico overzicht, de bevindingen vanuit Internal Audit, de input vanuit eerdere beveiligingsincidenten en bevindingen vanuit het privacy control framework meegenomen en gewogen. Het jaarplan wordt afgestemd met het Alliander Resilience Commissie.

De FG maakt jaarlijks een FG toezichtplan, voert dit uit en rapporteert periodiek over de naleving van privacy wet- en regelgeving binnen Alliander en over uitgevoerde onderzoeken.

Voor de inrichting, implementatie, uitvoering, beheer, monitoring en continue verbetering van Privacy binnen Alliander, wordt een Privacy Management Systeem ingericht en uitgevoerd, dat invulling geeft aan de belangrijkste eisen vanuit de Privacy Baseline[5]. Waar mogelijk integreert dit Privacy Management Systeem met het op vergelijkbare wijze ingevulde Information Security Management Systeem (ISMS).

3.1.4 Register van Verwerkingsactiviteiten

Doelstelling: Alliander heeft een duidelijk beeld van- en documenteert welke -persoonsgegevens worden verwerkt. Persoonsgegevens worden geïdentificeerd en er wordt op de juiste wijze mee omgegaan. In de maatregelen voor bescherming van persoonsgegevens wordt rekening gehouden met verschillen in de gevoeligheid van persoonsgegevens, de omvang van de verwerkingen de mogelijke impact voor betrokkene.

Om invulling te kunnen geven aan de verplichtingen die voortvloeien uit het verwerken van Persoonsgegevens, heeft Alliander een verwerkingsregister opgesteld, zoals genoemd in artikel 30 AVG. Verwerkingen worden op basis van Level 2 processen vastgelegd en opgenomen in het verwerkingsregister. Dit verwerkingsregister bevat:

- De naam en contactgegevens van Alliander of de betreffende entiteit, de FG en eventuele andere organisaties waarmee Alliander gezamenlijk Verwerkingsverantwoordelijke is;
- De doelen van de Verwerkingen;
- Een beschrijving van de categorieën van Betrokkenen en de categorieën Persoonsgegevens die worden verwerkt;
- Een beschrijving van de ontvangers van de Persoonsgegevens;
- Indien van toepassing, een beschrijving van het delen van Persoonsgegevens aan derde landen;
- De bewaartermijnen;
- Een algemene beschrijving van de technische en organisatorische beveiligingsmaatregelen.

De Privacy Officers beheren het verwerkingsregister. Proceseigenaren zijn verantwoordelijk voor het opnemen van (nieuwe) Verwerkingen in het register van verwerkingsactiviteiten op basis van geïdentificeerde Level 2 processen. Zij worden hierbij geadviseerd door de Privacy Officers. De FG controleert of het register van verwerkingsactiviteiten volledig en up-to-date is. Het register van verwerkingsactiviteiten wordt periodiek geactualiseerd. Eén keer per jaar richten de Privacy Officers zich tot de proceseigenaren met het verzoek om het register van verwerkingsactiviteiten te controleren op actualiteit en juistheden.

[5] https://www.cip-overheid.nl/media/1302/20190506-privacy-baseline-v3_2.pdf

3.1.5 Risicobeheersing en Data Privacy Impact Assessments

Doelstelling: De Privacy gerelateerde effecten van nieuwe processen, producten en diensten en het gebruik ervan binnen Alliander worden op systematische wijze geïdentificeerd, beoordeeld en aangepakt middels een Privacy Assessment.

Alliander hanteert een integrale en uniforme risico gebaseerde aanpak voor het adequaat beheersen van risico's voor betrokkenen op het gebied van Privacy; het Privacy Assessment. Dit betekent dat risico's op een eenduidige wijze worden geïnventariseerd en geclassificeerd. Bij het uitvoeren van een privacy risico analyse worden onder andere de volgende aspecten in ogenschouw genomen: rechtmatigheid van de verwerking, doelbinding, subsidiariteit en proportionaliteit en risico's voor de betrokken.

Er wordt maximaal gebruik gemaakt van bestaande kennis, producten, processen en overleggen die reeds eerder zijn ontwikkeld binnen de verschillende bedrijfsonderdelen om deze integraal in te zetten voor het Alliander Privacy beleid, richtlijnen en praktische handvaten.

Voor Alliander geldt dat voor een nieuwe Verwerking of een wijziging in een bestaande Verwerking een Business Impact Analyse (BIA) uitgevoerd dient te worden. Een BIA wordt door een Security Officer begeleidt en beoordeeld. Indien de Verwerking ook persoonsgegevens betreft wordt er in eerste instantie een Privacy Quick Assessment uitgevoerd. Op basis van de uitgevoerde Privacy Quick Assessment wordt bepaald of voor een afzonderlijke Verwerking een hoog risico bestaat en een DPIA noodzakelijk is. Een DPIA geeft inzicht in welke maatregelen getroffen moeten worden om het risico te verkleinen naar een minimaal en acceptabel niveau. Alliander beschikt over een standaard modellen voor een Privacy Quick Assessment en voor de uitvoering van een DPIA[6]. Proceseigenaren zijn verantwoordelijk voor de uitvoering van een Privacy Quick Assessment en eventueel de DPIA. Privacy Officers en Security Officers ondersteunen en adviseren bij de uitvoering hiervan. De FG geeft advies over de uitgevoerde DPIA.

De Privacy Officers houden een register bij van uitgevoerde DPIA´s en monitoren de voortgang van te implementeren beheersmaatregelen door de Proces-Eigenaar en rapporteren daarover aan de Corporate Privacy Officer en aan het lijnmanagement. Processen kunnen regelmatig worden aangepast. Dit kan ook effect hebben op de Verwerking van Persoonsgegevens. Als er een wijziging in het proces wordt doorgevoerd is het noodzakelijk om een eerder uitgevoerde DPIA te herzien en te kijken of de wijziging ook nieuwe risico's met zich meebrengt. Ook indien er geen proceswijzigingen worden doorgevoerd, is het noodzakelijk de uitgevoerde DPIA periodiek te herzien. De proceseigenaren zijn verantwoordelijk zijn voor de actualisering na drie jaar van de DPIA. Hiervan kan worden afgeweken indien blijkt dat het restrisico hoog is. Aan de hand van het netto risico wordt bepaald of de periodiciteit aangepast moet worden, de Privacy Officer en de FG adviseren over de eventuele verkorting van de periodiciteit in samenspraak.

[6] Voor Privacy Assessments worden door Alliander ten minste de volgende methoden gebruikt:

- De Privacy Quick Assessment voor Alliander intern;
- De DPIA template voor Alliander intern;
- De EDSN DPIA template voor sector processen;
- De Netbeheer Nederland template voor sector beoordelingen van slimme metergegevens toepassingen voor slim netbeheer

3.1.6 Privacy Architectuur (Gegevensbescherming door ontwerp en standaardinstellingen)

Doelstelling: Alliander neemt bij het ontwikkelen en wijzigen van producten, diensten, bedrijfssystemen of processen het Privacy beleid, de Privacy principes en/of de van toepassing zijnde wet- en regelgeving in acht.

Alliander past Privacy by design/default toe bij de (her)inrichting van processen en/of systemen en past, waar nodig, bestaande processen en/of systemen aan om deze in overeenstemming met de eisen in de AVG te brengen. Alliander stelt proceseigenaren, architecten, ontwerpers en bouwers in staat Privacy by design/default criteria toe te passen, als een uitwerking van het Alliander Privacy Beleid.

Bij de ontwikkeling, het ontwerp, selectie en het gebruik van toepassingen, diensten en producten waarbij persoonsgegevens worden verwerkt, houdt Alliander zo vroeg mogelijk in het ontwerpproces rekening met de Privacy principes en Privacy risico's. De beoordeling van Privacy risico's is een inherent en gedocumenteerd onderdeel van de projectmethodiek en/of het ontwikkelingsproces van Alliander.

Wanneer systemen, diensten en producten waarbij persoonsgegevens worden verwerkt Privacy-gerelateerde opties bieden, zijn deze standaard ingesteld op de meest beschermende optie met betrekking tot minimale dataverwerking (Privacy by default).

3.1.7 Beheer van Privacy Incidenten

Doelstelling: Alliander herkent incidenten met betrekking tot Privacy en handelt deze af. Op Privacy gerelateerde incidenten wordt adequaat gereageerd met het doel de gevolgen te beperken zowel voor betrokkene als voor Alliander en er worden maatregelen genomen om toekomstige inbreuken te voorkomen.

Binnen Alliander zijn procedures voor Datalekken ingericht en gepubliceerd[7]. Mogelijke Datalekken worden beoordeeld door een expert team. Afhankelijk van de aard en de omvang zal het expert team bestaan uit de Privacy Officer, de CPO, Privacy Jurist, de FG en de betrokken proces- of projectmanager, daar waar nodig aangevuld met andere experts.

De FG is vanuit zijn/haar rol gemachtigd om datalekken na beoordeling en uiterlijk binnen 72 uur na ontdekking te melden bij de Autoriteit Persoonsgegevens (AP). Een eventuele melding aan betrokkenen wordt gecoördineerd door de betrokken lijnmanagement in afstemming met de Manager Communicatie, de Privacy Officers en de FG. De FG informeert de Raad van Bestuur aangaande de melding bij de AP en eventuele melding aan betrokkenen

Een geconstateerd datalek kan aanleiding zijn voor de Privacy Officer of FG om (dringend) te adviseren om een proces of systeem tijdelijk te stoppen om de impact van het incident te beperken, waarbij de FG als escalatierichting dient indien het advies niet opgevolgd wordt. Het betrokken management kan het proces of systeem daarna weer hervatten, na het treffen van eventuele mitigerende maatregelen zoals vereist door de Privacy Officer en/of FG.

3.1.8 Competenties & Awareness

Doelstelling: Medewerkers zijn voldoende op de hoogte van de Privacy wet- en regelgeving, het Alliander Privacy Beleid en de richtlijnen binnen de organisatie, en hun verantwoordelijkheden met betrekking tot privacy. Alliander implementeert dit in de

[7] Procedure_Melden_Datalek_Alliander.v.1.0

werkprocessen en houdt programma's en acties om bewustwording te bereiken en op peil te houden.

Alliander borgt dat alle medewerkers een hoog niveau van bewustwording hebben op het gebied van privacy. In het kader daarvan is het lijnmanagement verantwoordelijk voor informerende en voorlichtende activiteiten op het gebied van privacy waarbij in ieder geval de meldplicht Datalekken een terugkerend onderwerp is. Medewerkers van alle lagen worden betrokken bij actuele privacy-issues en Datalekken om bewustwording te borgen.

Op het Alliander Intranet wordt informatie beschikbaar gemaakt over Privacy en informatiebeveiliging en worden o.a. handreikingen en templates beschikbaar gesteld. Bijvoorbeeld over de omgang met persoonsgegevens, privacy by design and default principes, een overzicht van de Privacy Officers en de te volgen procedure in geval van een mogelijk datalek.

3.1.9 Juridische toets van wijzigingen in wet- en regelgeving en/of bedrijfsvereisten

Doelstelling: Alliander houdt voldoende rekening met Privacy risico's die voortkomen uit veranderingen binnen Alliander (structuur en strategie), veranderende wet- en regelgeving en rechtspraak.

Door Juridische Zaken worden ten minste de volgende wettelijke eisen en regelingen gemonitord:

- Algemene Verordening Gegevensbescherming (AVG);
- De Uitvoeringswet AVG (UAVG);
- AP beleidsregels;
- Aanvullende richtlijnen vanuit de Europese Commissie
- EDPB Guidelines;
- Actuele rechtspraak op het gebied van Privacy

Interne communicatie van nieuwe en aankomende ontwikkelingen wordt door de Privacy Officer(s) verricht. Privacy ontwikkelingen kunnen aanleiding zijn om het Alliander Privacy Beleid te actualiseren.

Alliander zorgt er verder voor dat het effect op de Privacy vereisten gemonitord, beoordeeld en behandeld wordt, wanneer zich wijzigingen voordoen in:

- Overeenkomsten, waaronder gegevensuitwisselingsovereenkomsten met derden en verwerkersovereenkomsten;
- Bedrijfsactiviteiten en processen;
- Personele bezetting van functies en/of rollen die zijn belast met de verantwoordelijkheid voor Privacy en Security;
- Technologie (voordat deze wordt geïmplementeerd).

3.2 Informeren

3.2.1 Privacyverklaring

Doelstelling: Alliander informeert betrokkenen op transparante en begrijpelijke wijze over het beleid, de voorwaarden en activiteiten met betrekking tot het verzamelen, gebruiken, bewaren, verstrekken en verwijderen van persoonsgegevens.

Alliander dient Betrokkenen bij de verkrijging van de Persoonsgegevens te informeren over de Verwerking van de Persoonsgegevens Alliander heeft een privacy verklaring op haar websites waarin Betrokkenen worden geïnformeerd over de Verwerking van Persoonsgegevens door Alliander. Aanvullend op deze algemene berichtgeving worden Betrokkenen bij specifieke processen, waar mogelijk en noodzakelijk, aanvullend geïnformeerd over de betreffende gegevensverwerking. Bijvoorbeeld ten aanzien van het uitlezen van slimme meters.

Eventuele wijzigingen in de Privacy verklaringen worden door middel van een jaarlijks review proces opgepakt en gecommuniceerd, hiertoe behoren bijvoorbeeld nieuwe of gewijzigde doeleinden van de verwerking.

De Privacy verklaringen[8] die door Alliander worden opgesteld voldoen aan de vereisten in de UAVG en bevatten ten minste de volgende onderdelen:

- Verantwoordelijke voor de verwerking;
- Doel en grondslag voor verwerking; en
- Rechten van betrokkenen.

In de Privacyverklaring beschrijft Alliander onder meer op duidelijke en beknopte wijze:

- Welke keuzes de betrokkene heeft met betrekking tot de verzameling, het gebruik, en de verstrekking van persoonsgegevens;
- Wat de betrokkene moet doen om deze keuzes te maken;
- De mogelijkheid om de contactvoorkeuren aan te passen en hoe de betrokkene dit doet;
- Wat de gevolgen zijn als de persoonsgegevens die nodig zijn voor een transactie of dienst niet worden verstrekt;
- Wat de gevolgen zijn als de persoon weigert persoonsgegevens te verstrekken;
- Wat de gevolgen zijn van het niet verlenen of intrekken van toestemming.

3.3 Keuze en Toestemming

3.3.1 Toestemmingsraamwerk

Doelstelling: Alliander verkrijgt, indien vereist of noodzakelijk, toestemming van de betrokkene om persoonsgegevens te verwerken.

Wanneer een verwerking is gebaseerd op de grondslag toestemming:

- Verkrijgt en documenteert Alliander tijdig de toestemming van de betrokkene;
- Legt Alliander de voorkeuren van de betrokkene vast (schriftelijk of elektronisch);
- Documenteert Alliander wijzigingen in de contactvoorkeuren en verwerkt deze;
- Zorgt Alliander dat de voorkeuren van de betrokkene tijdig worden verwerkt;
- Bewaart Alliander de informatie om aan kunnen te tonen dat de toestemming is verleend.

Wanneer de verwerking van persoonsgegevens berust op toestemming, faciliteert Alliander de uitoefening van het recht van de betrokkene om zijn toestemming te allen tijde in te trekken.

3.4 Verzamelen

3.4.1 Minimale Gegevensverwerking

Doelstelling: De persoonsgegevens zijn toereikend, ter zake dienend en beperkt tot wat noodzakelijk is voor de gerechtvaardigde doeleinden waarvoor zij worden verwerkt

Alliander bepaalt bij iedere nieuwe verwerking welke persoonsgegevens noodzakelijk zijn voor het doel van de verwerking. Alliander zal de verwerking van persoonsgegevens beperken tot het voor het doel

[8] De Privacy verklaring t.b.v. medewerkers is instemming plichtig conform artikel 27 lid 1 sub k Wet op de Ondernemingsraden (WOR).

noodzakelijke minimum en periodiek nagaan of de verwerking van persoonsgegevens nog noodzakelijk is voor de producten en/of diensten van Alliander, of voor het uitvoeren van de interne bedrijfsprocessen.

3.5 Gebruiken, opslaan en verwijderen

3.5.1 Doelbinding

Doelstelling: Persoonsgegevens worden verwerkt en verzameld voor een welbepaald, uitdrukkelijk omschreven en gerechtvaardigd doel.

Alliander zal de verstrekking en het gebruik van persoonsgegevens beperken tot de gerechtvaardigde doeleinden en de betreffende wet- en regelgeving. Hierbij zal het doel welbepaald en uitdrukkelijk worden omschreven nog voordat de gegevensverwerking begint. Van alle gegevens zijn de rechtmatige gronden en de doeleinden van de verzameling en de verzameling welbepaald en uitdrukkelijk omschreven en gerechtvaardigd.

3.5.2 Bewaren van gegevens

Doelstelling: *Persoonsgegevens worden niet langer bewaard dan noodzakelijk is om het doel te bereiken waarvoor ze zijn verzameld of niet langer dan de bewaartermijn die (sectorspecifieke) wetgeving stelt.*

Alliander legt bewaartermijnen vast per categorie persoonsgegevens en bekrachtigt deze middels de Privacy Risico Eigenaar. Alliander documenteert het bewaarbeleid en de verwijderingsprocedures ten aanzien van persoonsgegevens en zorgt ervoor dat dat persoonsgegevens niet langer worden bewaard dan de vastgestelde bewaartermijn, tenzij er sprake is van een gerechtvaardigde reden of een wettelijke verplichting.

Gearchiveerde kopieën en back-ups dienen bewaard en verwijderd overeenkomstig het bewaarbeleid. Alliander instrueert verwerkers over de gestelde bewaartermijnen.

3.5.3 Verwijdering en anonimiseren

Doelstelling: Persoonsgegevens worden indien nodig geanonimiseerd en/of verwijderd binnen Alliander. Voor anonimiseren geldt dat de identiteit van personen niet kan worden herleid of afgeleid en persoonsgegevens niet meer beschikbaar zijn nadat de bewaartermijn is verstreken.

Alliander heeft voorzieningen ingericht om te waarborgen dat het verwijderen van persoonsgegevens geschiedt conform het vastgestelde bewaarbeleid, ongeacht de vorm of media waarin deze zijn opgeslagen. Het bewaarbeleid omvat de verwijdering van originele, gearchiveerde gegevens, back-ups. De verwijdering van persoonsgegevens wordt vastgelegd door gebruik te maken van auditlogs. Het bewaarbeleid wordt vastgesteld door de Privacy Risico Eigenaar van het betreffende data-domein.

3.5.4 Gebruik en beperking

Doelstelling: Persoonsgegevens worden niet verwerkt als de betrokkene een beperking van de verwerking heeft verkregen. Bezwaren van de betrokkene tegen de verwerking van persoonsgegevens worden op een adequate wijze afgehandeld.

Alliander heeft processen ingericht om adequaat te handelen wanneer betrokkenen hun recht op beperking van of bezwaar tegen de verwerking uitoefenen.

3.6 Rechten van betrokkenen

3.6.1 Afhandelen van verzoeken

Doelstelling: Verzoeken en bezwaren van betrokkenen wordt conform vastgestelde werkinstructies afgehandeld, op een wijze die invulling geeft aan de wettelijke verplichtingen en behandelingstermijnen.

Betrokkenen van wie Alliander Persoonsgegevens verwerkt, hebben volgens de wet bepaalde rechten waarmee zij controle kunnen uitoefenen op de Verwerking van hun Persoonsgegevens.
Alliander onderschrijft deze rechten en zal ook aan de verzoeken van Betrokkenen omtrent deze rechten voldoen. In de privacy statements wordt verwezen naar de volgende rechten:

- U heeft recht op inzage van de Persoonsgegevens die wij van u verwerken.
- U heeft recht op informatie over de wijze waarop wij uw Persoonsgegevens verwerken.
- U heeft recht op correctie of aanvulling van uw Persoonsgegevens.
- U heeft het recht om uw Persoonsgegevens te laten verwijderen.
- U heeft het recht om minder Persoonsgegevens te laten verwerken.
- U kunt bezwaar maken tegen de Verwerking van uw Persoonsgegevens.
- U heeft het recht ons te verzoeken uw Persoonsgegevens in een gestructureerde, gangbare en machine-leesbare vorm aan u over te dragen.
- U kunt bezwaar maken tegen geautomatiseerde individuele besluitvorming.

Verzoeken en bezwaren van klanten worden zo spoedig mogelijk afgehandeld via het Klant Contact Center. Verzoeken en bezwaren van medewerkers worden afgehandeld via de HR Servicedesk. Alliander verifieert altijd de identiteit van de betrokkene alvorens een verzoek of bezwaar in behandeling te nemen.

De juiste wijze van afhandeling, de termijnen hiervoor en de wijze van verificatie zijn vastgelegd in werkinstructies van respectievelijk het Klant Contact Center en de HR Servicedesk. Uitgangspunt is dat standaard verzoeken en bezwaren binnen een periode van 1 maand worden afgehandeld, voor complexe verzoeken en bezwaren geldt een afhandelingstermijn van maximaal 8 weken. Indien na eerste analyse blijkt dat een verzoek of bezwaar complex is, wordt de betrokkene op de hoogte gesteld van de complexiteit van het verzoek of bezwaar en wordt gemeld dat de afhandelingstermijn 2 maanden is i.p.v. 1 maand.

Voor de persoonsgegevens waarvan Alliander niet de bronhouder is (d.w.z. dat de persoonsgegevens door een toeleverancier aan Alliander verstrekt zijn ter ondersteuning van het leveren van een dienst) kan Alliander mogelijk het verzoek niet uitvoeren. Alliander stelt de betrokkene op de hoogte en geeft de naam van de bronhouder (toeleverancier) door.

Klachten met betrekking tot Privacy worden behandeld via het standaard proces bij het Klant Contact Center waarbij de Privacy Officers betrokken kunnen worden en indien nodig de FG.

3.7 Juistheid en volledigheid van gegevens

Doelstelling: Vastgelegde procedures voor het valideren, aanpassen en bijwerken van persoonsgegevens waarborgen de juistheid en volledigheid van persoonsgegevens.

Alliander heeft procedures opgesteld om persoonsgegevens aan te passen en te valideren wanneer deze worden verzameld, gecreëerd, bijgehouden en bijgewerkt. Volgens deze procedures wordt de datum vastgelegd waarop de persoonsgegevens zijn verkregen of bijgewerkt en wordt gespecificeerd wanneer de persoonsgegevens niet meer geldig zijn. Tevens is vastgelegd wanneer en hoe persoonsgegevens dienen te worden bijgewerkt en wat de bron is voor de bijwerking

Alliander verifieert de juistheid en volledigheid van persoonsgegevens die zijn verkregen van de betrokkene of van derden, of die zijn verstrekt aan derden en waarborgt dat de verwerkte persoonsgegevens juist en volledig genoeg zijn om beslissingen op te baseren.

Alliander voert periodiek steekproeven uit om de juistheid van persoonsgegevens te controleren en, wanneer de steekproeven hier aanleiding toe geven, deze zo nodig verder te beoordelen en te corrigeren.

3.8 Doorgifte Persoonsgegevens

3.8.1 Verstrekken aan derden en registratie

Doelstelling: Persoonsgegevens worden niet aan derden verstrekt zonder wettelijke basis of voor andere doeleinden dan waarover de betrokkene is geïnformeerd

Alliander heeft procedures ingericht om te voorkomen dat persoonsgegevens aan derden worden verstrekt, indien de wettelijke basis daarvoor ontbreekt en/of de betrokkene daarover niet is geïnformeerd.

Alliander documenteert wat de aard van de persoonsgegevens is die aan derden worden verstrekt en in welke mate deze worden verstrekt en monitort of de verstrekking aan derden nog steeds in overeenstemming is met het Alliander Privacy Beleid, of uitdrukkelijk is toegestaan of verplicht is op grond van wet- of regelgeving.

In beginsel worden persoonsgegevens alleen aan derden verstrekt voor gerechtvaardigde doeleinden.

3.8.2 Overeenkomsten met derden

Doelstelling: Bij de verwerving van oplossingen en diensten (gerelateerd zijnde aan persoonsgegevens) van derden wordt voldoende aandacht besteed aan Privacyoverwegingen en -vereisten, waardoor geborgd wordt op de juiste wijze met persoonsgegevens wordt omgegaan en deze worden beschermd.

Bij een gezamenlijke of gedeelde verantwoordelijkheid in een keten wordt in een onderlinge regeling, zoals bedoeld in de AVG, afgesproken op welke wijze persoonsgegevens zorgvuldig worden verwerkt.

Met elke verwerker wordt een verwerkersovereenkomst afgesloten. Daarin wordt onder meer het auditrecht, beveiligingsmaatregelen en een procedure voor datalekken afgesproken. Subverwerkers zijn alleen toegestaan indien er een verwerkersovereenkomst met de verwerker is en uitsluitend na schriftelijke toestemming van Alliander.

Wanneer er een noodzaak bestaat om persoonsgegevens uit te wisselen waarbij zowel Alliander als de andere partij verwerkingsverantwoordelijke is, kan een Gegevensuitwisselingsovereenkomst (GUO) of een gelijkwaardige overeenkomst tussen partijen afgesloten worden.

Uitgangspunt is dat verwerking van persoonsgegevens plaats vindt binnen de Europese Economische Ruimte (EER) door een in de EER gevestigde contractspartij, die niet verplicht kan worden tot afgifte van gegevens aan niet-Europese overheden. Wanneer verwerking van persoonsgegevens buiten de EER plaats moet vinden en het land niet door de EC beoordeeld passende beschermingsniveau beschikt, dan worden de toepasselijke EU-modelcontractclausules overeengekomen en worden andere passende maatregelen genomen zoals encryptie en pseudonimisering.

3.9 Beveiliging van de verwerking van persoonsgegevens

3.9.1 Programma informatiebeveiliging

Doelstelling: Persoonsgegevens worden adequaat beschermd tegen onopzettelijke fouten of verlies, of kwaadwillige handelingen zoals hacken, diefstal, ongeautoriseerde toegang, verstrekking of verlies.

Het beveiligen van persoonsgegevens wordt geadresseerd in het Informatiebeveiligingsbeleid. Door middel van een Beschikbaarheid-, Integriteit- en Vertrouwelijkheid analyse wordt bepaald welke IT-systemen verhoogde aandacht krijgen wat beveiligingsmaatregelen betreft, onder andere vanwege de persoonsgegevens die verwerkt of opgeslagen worden in het betreffende systeem.

3.9.2 Identiteit en toegangsbeheer

Doelstelling: Toegangsrechten worden adequaat toegekend, gewijzigd en ingetrokken. Dit verkleint de kans op ongeautoriseerde toegang tot en onjuiste verwerking van persoonsgegevens, of inbreuk in verband met persoonsgegevens door interne medewerkers, derden of hackers.

Alliander heeft technische en organisatorische maatregelen ingericht om vast te stellen in hoeverre en op welke wijze gebruikers toegang krijgen tot persoonsgegevens en deze gebruikers te identificeren en te authentiseren voordat toegang wordt verleend tot systemen die persoonsgegevens verwerken. Dit is gebaseerd op de gevoeligheid van de gegevens en de gerechtvaardigde zakelijke doeleinden van de gebruikers op basis van het “need-to-know” principe. De toegang tot persoonsgegevens wordt vastgelegd op rol- en functie niveau en wordt minimaal jaarlijks getoetst op juistheid.

3.9.3 Veilige gegevensoverdracht

Doelstelling: Door beperkte toegang tot persoonsgegevens tijdens verzending wordt op adequate wijze ongeautoriseerde verstrekking, inbreuk, wijziging of verwijdering van persoonsgegevens voorkomen.

Alliander beschermt persoonsgegevens die, in zowel fysieke als elektronische vorm, worden verstuurd per elektronisch netwerk, post, koerier of andere methoden, tegen ongeautoriseerde toegang en invloeden. Alliander heeft hiertoe technische en organisatorische maatregelen ingericht om een passend niveau van beveiliging te borgen voor de verzending en ontvangst van persoonsgegevens. Waarbij voor elektronische verzending versleutelingstechnologie wordt toegepast die voldoet aan de stand der techniek.

3.9.4 Versleuteling en eindpuntbeveiliging

Doelstelling: Inbreuken in verband met persoonsgegevens (onopzettelijk verlies of kwaadwillige handelingen zoals diefstal, ongeautoriseerde verstrekking of verlies) worden voorkomen door middel van versleuteling.

Opslag van persoonsgegevens op draagbare media of apparaten is niet toegestaan, tenzij er sprake is van zakelijke noodzaak en de opslag is goedgekeurd door het management. Indien persoonsgegevens zijn opgeslagen op draagbare media of apparaten, is versleutelingstechnologie toegepast die de standaard is in de sector.

Wanneer het dienstverband van medewerkers of overeenkomsten met derden worden beëindigd, zijn er procedures voor het terughalen en vernietigen van draagbare media en apparaten die gebruikt zijn om toegang te verkrijgen tot of opslaan van persoonsgegevens, of voor het permanent wissen van (persoons)gegevens van de draagbare media en apparaten en deze opnieuw in te zetten.

3.9.5 Registreren van toegang

Doelstelling: Toegang of toegangspogingen tot persoonsgegevens door medewerkers en derden worden geregistreerd en onderzocht om (pogingen tot) inbreuk op de beveiliging van persoonsgegevens te detecteren en te voorkomen.

Alliander heeft systemen en procedures ingericht om de logische en fysieke toegang tot persoonsgegevens te beheren en de toegang hiertoe te registreren en te monitoren. De logbestanden bevat voldoende details en wordt lang genoeg bewaard om de gegevens te kunnen analyseren en onderzoeken op het ongeautoriseerd of onopzettelijk vernietigen of verliezen van persoonsgegevens en op ongeautoriseerde toegang tot persoonsgegevens en pogingen om ongeautoriseerde toegang te verkrijgen.

3.9.6 Testdata

Doelstelling: Persoonsgegevens worden niet in origineel formaat gebruikt voor testdoeleinden, en worden verwijderd, geanonimiseerd of gepseudonimiseerd in test datasets.

Voor het uitvoeren van testen worden geen productiegegevens gebruikt van daadwerkelijke betrokkenen. Testdata sets bestaan derhalve uit gefingeerde gegevens.

Wanneer het gebruik van productiegegevens waaronder persoonsgegevens niet vermeden kan worden dient er een risicoanalyse uitgevoerd te worden in de vorm van een DPIA voorzien van bijbehorende advies op onderstaande onderwerpen:

- Wanneer wordt getest (tijdstippen en duur);
- Wat wordt er getest (op welke onderdelen);
- Waar wordt getest (is de locatie en de overdracht veilig);
- Met hoeveel en welke persoonsgegevens wordt getest (niet meer dan noodzakelijk);
- Wie test (beperkte groep medewerkers);
- Hoe alles wordt gelogd (toezicht en verantwoording);
- Welke (extra) Securitymaatregelen zijn genomen om Privacy van betrokkenen te garanderen;
- Wat er gebeurt na het testen met de resultaten, de persoonsgegevens en het testrapport (verspreiding, opslag, bewaartermijnen, vernietiging).

De Functionaris Gegevensbescherming heeft toezicht hierop en kan er desgewenst over adviseren. Daarna valt een definitief schriftelijk besluit door de beslissingsbevoegde. Dit besluit en bijbehorende argumentatie, testplan, werkwijze en evaluatie worden gearchiveerd.

3.10 Intern Toezicht

3.10.1 Beoordeling van compliance met Alliander Privacy Beleid en wet- en regelgeving.

Doelstelling: Adequaat toezicht op de interne organisatie en derden waarborgt dat de organisatie voldoet aan het Alliander Privacy Beleid en de wet- en regelgeving met betrekking tot Privacy en vermindert het risico op inbreuk in verband met persoonsgegevens of verlies hiervan

Alliander beoordeelt periodiek de naleving van het Alliander Privacy Beleid, de afgeleide procedures en richtlijnen en verplichtingen vanuit geldende wet- en regelgeving, middels de door Alliander opgestelde normenkaders en beheersinstrumenten zoals de KICU en het Business Control Framework Privacy. De FG voert tevens zo nodig zelfstandig controle activiteiten uit en/of dient bij de afdeling Internal Audit verzoeken in voor Privacy audits gericht op specifieke aspecten of processen.

Deze periodieke beoordelingen worden gedocumenteerd en gerapporteerd aan het lijnmanagement . De resultaten van de conformiteitsbeoordeling en aanbevelingen voor verbetering worden aan het lijnmanagement gerapporteerd en middels een verbeterplan geïmplementeerd. De betrokken proceseigenaar is verantwoordelijk voor het oplossen van bevindingen of tekortkomingen.

De resultaten van de conformiteitsbeoordeling en aanbevelingen voor verbetering worden gemonitord vanuit het Privacy Management Systeem, om te waarborgen dat tijdig passende corrigerende maatregelen worden genomen, waaronder zo nodig de herziening van het Privacy beleid en procedures.

3.10.2 Periodiek monitoren van Privacy beheersmaatregelen

Doelstelling: Systematische en periodieke evaluatie van Privacy processen en beheersmaatregelen waarborgt dat deze naar behoren werken, zodat blijvend wordt voldaan aan de van toepassing zijnde wet- en regelgeving.

Het lijnmanagement van Alliander evalueert, volgens een vooraf gesteld plan, de doeltreffendheid van de beheersmaatregelen zoals gesteld in de DPIA's.

Alliander beslist op basis van de gevoeligheid van de betreffende persoonsgegevens en het risico op blootstelling of verlies welke beheersmaatregelen worden gemonitord, beoordeeld en/of gecontroleerd, hoe en met welke frequentie dit gebeurt. Dit betreft ook de derde partijen die als verwerker persoonsgegevens verwerken namens Alliander; als onderdeel van het contractmanagementproces worden derde partijen gemonitord, beoordeeld en/of gecontroleerd.

De uitvoering en documentatie van deze evaluatie is onderdeel van de KICU en het Business Control Framework. Vanuit het Privacy Management Systeem wordt gewaarborgd dat het monitoren resulteert in herstel van tekortkomingen en continue verbetering.

4 Governance

In de volgende paragrafen worden de governance en bijbehorende verantwoordelijkheden, taken en bevoegdheden van de rollen beschreven. Hierbij wordt gebruik gemaakt van het RASCI-model.

4.1 RASCI model

- **(R)esponsible**: Degene die verantwoordelijk is voor de uitvoering. Verantwoording wordt afgelegd aan de persoon die accountable is.
- **(A)ccountable**: Degene die (eind)verantwoordelijk, bevoegd is en goedkeuring geeft aan het resultaat. Als het erom gaat, moet hij/zij het eindoordeel kunnen vellen, vetorecht hebben.
- **(S)upportive**: Degene die ondersteuning verleent aan het proces, project of lijnwerkzaamheden.
- **(C)onsulted**: Deze persoon geeft (mede) richting aan het resultaat, hij/zij wordt voorafgaand aan beslissingen of acties geraadpleegd en er vindt terugkoppeling hierover plaats. Dit is tweerichtingscommunicatie.
- **(I)nformed**: Degene die geïnformeerd wordt over het proces, de beslissingen, over de voortgang, bereikte resultaten enz. Dit is eenrichtingscommunicatie.

4.2 Three lines model

Alliander hanteert het “three lines” model voor risicobeheersing. Dit model houdt het volgende in:

- **1e lijn – Lijnmanagement**: Het management is verantwoordelijk voor het managen van risico’s en voert dagelijks impliciet en expliciet werkzaamheden uit aangaande het beheersen en/ of accepteren van risico’s. Het lijnmanagement rapporteert in de hiërarchische lijn over Privacy risico’s.
- **2e lijn – Ondersteunende staven**: De stafafdelingen ondersteunen het management met het uitzetten van de risicomanagement strategie, beleid en werkzaamheden. Daarnaast zien zij toe op de implementatie, met inbegrip van een adequate risicobeheersing, en rapporteren hierover aan de Raad van Bestuur.
- **3e lijn – Internal Audit**: De afdeling Internal Audit maakt geen onderdeel uit van het primaire proces en geeft onafhankelijke zekerheid aan de directie en/of Raad van Bestuur. Indien gewenst kan een externe auditor, in afstemming met Internal Audit, controles uitvoeren.

De werkzaamheden in het kader van monitoring en toetsing vinden plaats in afstemming tussen de 2^{e} en 3^{e} lijn. Hierdoor ontstaat een eenduidige monitoringslijn en worden dubbele controles voorkomen.

4.3 Data Governance Model

De Raad van Bestuur is eindverantwoordelijk, echter de operationele verantwoordelijkheid wordt binnen de organisatie-eenheden belegd. Het proces én data eigenaarschap ligt bij de 1^{e} lijnorganisatie en wordt gedefinieerd en vastgelegd in het 1Alliander Proces Model. Iedere bewerking die plaatsvindt op data leidt tot eigenaarschap over die bewerking en de resulterende data uit die bewerking. Er is ook altijd een initiële verwerking, het creëren of voor het eerst opslaan van deze data binnen Alliander, waardoor er altijd een (oorspronkelijke) Data-Eigenaar is aan te wijzen. Indien de data persoonsgegevens betreft is de Data-Eigenaar tevens Privacy Risico Eigenaar. De Privacy Risico Eigenaar is verantwoordelijk voor het scheppen van de juiste kaders en technische en organisatorische voorwaarden voor het (verder) verwerken van de persoonsgegevens.

Bovenstaand proces verloopt via de Data Governance zoals die door het Data Office wordt ingericht en wordt ondersteund door de Privacy Officers, die de Privacy Risico Eigenaar adviseren en tevens de product owners / projectleiders voorzien van Privacy by Design kaders om in een vroeg stadium in de ontwikkeling al rekening te houden met bepaalde Privacy vereisten. Zoals juiste onderbouwing voor het gebruik van persoonsgegevens, dataminimalisatie en life-cycle-management.

4.4 Afwijken van het beleid (Comply or Explain)

De Privacy Risico Eigenaar heeft de mogelijkheid om af te (laten) wijken van het beleid. Een rechtvaardiging hiervoor kan zijn dat de kosten, indien het beleid gevolgd wordt, hoger uitvallen dan de mogelijke schade bij manifest worden van het risico. Het "*Comply or Explain*" principe wordt gehanteerd, met dien verstande dat alle afwijkingen formeel worden geaccepteerd door de Privacy Risico-eigenaar, geregistreerd en gemonitord door de betreffende Privacy Officer en gerapporteerd via de rapportagelijn aan de CPO/FG en de Raad van Bestuur.

4.5 Rollen en functies binnen de Alliander organisatie

Raad van Bestuur (CEO, CFO, CTO en COO) - Accountable
De Raad van Bestuur stelt de risicobereidheid en het Alliander Privacy Beleid vast en delegeert de uitvoering van het beleid hiervan aan de directeuren van de organisatie-eenheden. De Raad van Bestuur is eindverantwoordelijk voor het beheersen van Privacy risico's binnen Alliander en stelt vast dat het beleid daadwerkelijk wordt uitgevoerd. Daarnaast benoemt de Raad van Bestuur de Functionaris Gegevensbescherming (FG) en mandateert deze om toe te zien op de naleving van de Privacy wetgeving.

Lijnmanagement - Responsible
Het lijnmanagement vervult de 1e lijn functie in het "three lines" model en is verantwoordelijk voor de risicobeheersing en voor de naleving en uitvoering van het Alliander Privacy Beleid. Het lijnmanagement zorgt binnen de organisatie-eenheden ervoor dat:

- De organisatie in staat is om de gedelegeerde verantwoordelijkheden te dragen;
- Het Alliander Privacy Beleid wordt uitgedragen, en in woord en daad ondersteund;
- Privacy risico's worden gesignaleerd en geadresseerd en deze worden voorgelegd aan de Privacy Risico Eigenaar;
- Gerapporteerd wordt over de beheersing van de Privacy risico's aan de Raad van Bestuur;
- Normen en beheersmaatregelen zoals gesteld door de Privacy Risico Eigenaar worden uitgevoerd die op verwerkingen van persoonsgegevens van toepassing zijn;
- De noodzakelijke capaciteit wordt ingezet om de Privacy en Security maatregelen te kunnen waarborgen;
- De 1e lijn controle op Privacy binnen de organisatie is gewaarborgd;
- Bewustwording ("awareness") van medewerkers wordt bevorderd op het gebied van Privacy.

Privacy Risico Eigenaar - Responsible
Vanuit de AVG is er de verplichting om voor iedere (verdere) verwerking van persoonsgegevens een de rechtmatigheid van de Verwerking te toetsten aan de hand van de initiële verwerking bij de bron (Grondslag en Doelbinding). Het beleggen van eindverantwoordelijkheid in de vorm van Privacy Risico Eigenaarschap bij een Organisatie-eenheid is essentieel. Waar het Privacy Risico Eigenaarschap valt, wordt bepaald door het startpunt in de keten waarvoor de data (voor het eerst) wordt ontsloten vanuit de bron (bron systeem of sleutel register). De Privacy Risico Eigenaar is verantwoordelijk voor het scheppen van de juiste kaders en voorwaarden voor het (verder) verwerken van de data.
De Privacy Risico Eigenaar is verantwoordelijkheid voor:

- De juiste risico afweging ten aanzien van verdere verwerking van Persoonsgegevens binnen de organisatie en het vereisen van beheersmaatregelen ten aanzien van voorgenomen verwerkingen
- Het accepteren van het eventuele rest-risico en het vaststellen van de DPIA.

Privacy Officer - Consulted
Het lijnmanagement en de Privacy Risico Eigenaar wordt in de uitvoering van haar taken ondersteund door één of meerdere Privacy Officers, die een adviserende en ondersteunende taak hebben. De Privacy Officer heeft op het gebied van Privacy, de volgende taken, verantwoordelijkheden en bevoegdheden:

- Vertalen van het Alliander Privacy Beleid naar specifieke richtlijnen voor het organisatie onderdeel;
- Toezicht op handhaving van toepasselijke wet- en regelgeving en naleving van het Alliander Privacy Beleid en richtlijnen binnen projecten en programma's. Indien noodzakelijk,

bijvoorbeeld in het geval van onrechtmatige verwerkingen, kan de Privacy Officer escaleren naar de Corporate Privacy Officer, de Functionaris Gegegevensbescherming en/of het lijnmanagement en de Privacy Risico Eigenaar;

- Deelnemen aan het Alliander Privacy overleg;
- Ondersteunen van het lijnmanagement bij het borgen van de continue verbetercyclus (PDCA) o.a. door:
    - begeleiding bij het opstellen van het Privacy plan en de jaarlijkse revisie daarop;
    - begeleiding bij het uitvoeren van de technische en organisatorische maatregelen;
- Rapporteren binnen de risicobeheersingslijn over Privacy aan de het lijnmanagement en de Privacy Risico Eigenaar;
- Uitvoeren van Privacy Assessments en het inzichtelijk maken van Privacy risico's ter besluitvorming over acceptatie dan wel mitigatie door de Privacy Risico eigenaar.
- Ondersteunen van het lijnmanagement en de medewerkers met kennis over Privacy zodat zij hun verantwoordelijkheid op dit gebied juist kunnen invullen (awareness);
- Aanspreekpunt ten aanzien van het data-domein op het gebied van Privacy;
- Op de hoogte zijn van externe invloeden die van invloed kunnen zijn op de Privacy activiteiten;
- Draagt bij aan de centrale registratie bij van Privacy incidenten in een incidentenregister en is verantwoordelijk voor het (laten) opvolgen en rapporteren over Privacy incidenten aan het lijnmanagement en de Privacy Risico Eigenaar;
- Coördineren en faciliteren van in- en externe Privacy audits en eventuele certificeringen.
- Rapporteren over audit bevindingen op het gebied van Privacy aan het lijnmanagement en de Privacy risico-eigenaar.

Corporate Privacy Officer – Consulted / Informed

De Corporate Privacy Officer heeft een 2e lijns functie binnen in het "three lines" model van risicobeheersing. De Corporate Privacy Officer is verantwoordelijk voor:

- Het coördineren van het Alliander Privacy Beleid in opdracht van de Raad van Bestuur;
- Het monitoren van veranderingen in wetgeving en tijdig vertalen hiervan naar impact op Alliander (beleid);
- Samenbrengen van de verschillende Privacy activiteiten en functionarissen binnen Alliander;
- Ondersteunen van lijnmanagement en Privacy Officers, middels gevraagd en ongevraagd advies over het beheersen van de Privacy risico's;
- Is op de hoogte van externe invloeden, neemt hiervoor ook deel aan relevante werkgroepen en discussies buiten Alliander en deelt deze binnen Alliander;
- Verbinding zoeken met de overige Corporate Control disciplines zoals Risicomanagement en Compliance, Crisismanagement en overige stakeholders zoals de CISO en het Data Office;
- Toezien op de implementatie en toetsing hierop van adequate risicobeheersing op het gebied van Privacy en rapportering hierover aan de Raad van Bestuur via de ARC.

Functionaris Gegevensbescherming – Consulted / Informed

Het is een wettelijke verplichting voor Alliander om een Functionaris Gegevensbescherming (FG) aan te stellen. Alliander heeft een FG in dienst. Contactgegevens van de FG staan vermeld op de website van Alliander en Liander. De FG is een onafhankelijke toezichthouder die gevraagd en ongevraagd advies geeft op het gebied van de AVG. Om de FG in staat te stellen deze adviesrol te vervullen wordt alle relevante informatie tijdig met de FG gedeeld, zodat hij/zij passend advies kan verlenen. Advisering door de FG is niet vrijblijvend. Op een door de FG uitgebracht advies wordt binnen 5 werkdagen een reactie gegeven door de geadresseerde van het advies. Wanneer het advies van de FG niet wordt gevolgd, laat de geadresseerde van het advies dit met redenen omkleed weten aan de FG. De FG krijgt de kans om zijn/haar afwijkende mening duidelijk te maken aan de verwerkingsverantwoordelijke.

De FG heeft de volgende wettelijke taken:

- De FG informeert en adviseert over de verplichtingen op grond van de (U)AVG

- De FG ziet toe op de naleving van de (U)AVG en het Alliander Privacy Beleid
- De FG geeft gevraagd en ongevraagd advies over de uitvoering van Privacy Assessments en ziet toe op de uitvoering hiervan
- De FG werkt samen en treedt op als contactpunt voor de Autoriteit Persoonsgegevens.
- De FG rapporteert jaarlijks over de uitvoering van haar taken richting de hoogste orgaan binnen de organisatie

De FG is de schakel tussen Alliander en de Autoriteit Persoonsgegevens. Hoewel de FG gehouden is tot geheimhouding, dan wel vertrouwelijkheid met betrekking tot de uitvoering van haar taken, belet dat deze niet om met de Autoriteit Persoonsgegevens overleg te plegen en advies te vragen omtrent de uitleg van bepaalde onderdelen van de (U)AVG.

Privacy Jurist - Consulted
De Privacy Jurist is een 2e lijns functie binnen in het “three lines” model van risicobeheersing en geeft gevraagd en ongevraagd advies op het gebied van Privacy wet- en regelgeving. Dit is eveneens gericht op het monitoren van nieuwe en gewijzigde wet- en regelgeving en de potentiële impact hiervan voor Alliander.

Data Office – Consulted / Informed
Het Data Office is erop gericht de datastrategie effectief om te zetten naar visie en beleid en middels de data governance in te bedden in de organisatie zodat data vindbaar, toegankelijk, (her)bruikbaar en uitwisselbaar is.

Internal audit (IA) - Informed
IA is een onafhankelijke functie die aanvullende zekerheid verschaft aan het management van Alliander, en met name de Raad van Bestuur, omtrent de beheersing, effectiviteit, efficiency en compliance van de bedrijfsvoering. In dit kader evalueert IA systematisch de processen met betrekking tot beheersing, risicomanagement en besturing (governance). Hierdoor draagt IA bij aan de verbetering van de bedrijfsvoering en het bereiken van de doelstellingen van Alliander. IA vervult de 3e lijn functie in het “three lines” model van risicobeheersing.

Alliander medewerker - Informed
De mate waarin Privacy risico’s beheerst worden is grotendeels afhankelijk van de mate waarin de Alliander medewerker het Alliander Privacy Beleid (en richtlijnen en handboeken) naleeft, bewust is van risico’s en daar naar kan handelen, en incidenten tijdig meldt.

Ondernemingsraad - - Consulted / Informed
Een ondernemingsraad heeft volgens artikel 27, lid 1k WOR instemmingsrecht op regelingen die impact hebben op de Privacy van medewerkers.

4.6 Overleggremia

Strategisch - Alliander Resilience Committee (ARC)
Binnen de Raad van Bestuur valt de integrale risicobeheersing, waaronder dus ook Privacy, onder de portefeuille van de Chief Financial Officer (CFO). Het doel van de Alliander Resilience Committee (ARC) is het strategisch ondersteunen van het management proces voor de disciplines Privacy, Security, business continuity en data governance en het informeren en adviseren van de Raad van Bestuur Alliander over het bestaan en de werking van het Privacy en Security management systeem en beheersing van de Privacy en Security risico’s. Aspecten die invulling geven aan dit doel zijn:

- Horizontaal platform bieden voor informatie- en kennisuitwisseling tussen de deelnemende organisatie onderdelen en betreffende staven;
- Voorbereidend orgaan voor de Raad van Bestuur voor besluitvorming over het Alliander Privacy Beleid;

- Duiden van het eigenaarschap voor Privacy risico's die naar hun aard en inhoud meerdere bedrijfsonderdelen raken en niet bij een individueel bedrijfsonderdeel horen;
- Voorbereiden van besluitvorming voor de Raad van Bestuur rondom Privacy risico's die meerdere bedrijfsonderdelen raken;
- Het bevorderen van aanbevelingen op het gebied van ontwikkeling van risicomanagement;
- Opdracht gevend voor Alliander brede initiatieven op het gebied van Privacy;
- Informeren over Alliander brede zaken, zoals aanpassingen in wet- en regelgeving;
- Het informeren en adviseren van de Raad van Bestuur van Alliander over het bestaan en de werking van het Privacy & Security management systeem.

Tactisch - Alliander Privacy Overleg (APO)
Privacy maakt een integraal onderdeel uit van verschillende bedrijfsprocessen. Dagelijks zijn diverse functionarissen binnen Alliander bezig met het uitvoeren, monitoren en optimaliseren van privacy en dataprotectie. Samenwerking en afstemming zijn daarbij cruciale succesfactoren.

- Doel van het APO is om de genoemde samenwerking en afstemming mogelijk te maken op een gestructureerde en geborgde wijze. Het overleg is (beleids)voorbereidend voor het ARC.
- Onderwerpen die o.a. besproken worden in de APO zijn: afstemming over beleid, kennisuitwisseling over relevante onderwerpen en nieuwe ontwikkelingen, informeren over status projecten en activiteiten en evaluatie van incidenten.
- Deelnemers aan het overleg zijn: Corporate Privacy Officer, de FG en de Privacy Officers van de organisatieonderdelen. Daarnaast kunnen personen op ad hoc basis uitgenodigd worden al naar gelang de agenda van het overleg.

4.7 Naleving van het beleid

Controle op de naleving van het beleid is noodzakelijk om te borgen dat Privacy risico's in voldoende mate beheerst worden. Om uitvoering te geven aan het beleid en de daarin gestelde maatregelen is een hiërarchie aan controlemechanismen te onderkennen:

- Zelfcontrole (1e lijn). Elke medewerker is verantwoordelijk om het beleid en maatregelen na te leven;
- Controle door management (1e lijn). Het management heeft de verantwoordelijkheid om te controleren dat de medewerkers het beleid naleven.
- Interne controle door Privacy Officer (1e lijn). De Privacy Officer evalueert, stelt bij en controleert de naleving van het beleid en de maatregelen binnen het bedrijfsonderdeel.
- Interne monitoring en controle Alliander (2e lijn). De CPO/FG evalueert, stelt bij en monitort de naleving van het beleid en richtlijnen binnen Alliander. Zij doet dit primair op basis van eerstelijns rapportages. Daarnaast toetst de CPO/FG zaken onafhankelijk via het Business Control Framework Privacy ten behoeve van de Raad van Bestuur/directie.
- Interne controle (3e lijn). Internal Audit voert audits uit op basis van het risico gebaseerde jaarplan of indien de omstandigheden daar om vragen. Doel hiervan is om voor specifieke thema's, systemen of processen aanvullende *assurance* te verstrekken.
- Externe controle. Indien gewenst kan periodiek middels een externe auditor het beleid en maatregelen getoetst worden in opzet, bestaan en werking. De resultaten worden afgestemd met Internal Audit en de FG en aangeboden aan de het lijnmanagement en de betreffende Privacy Risico Eigenaar.

BIJLAGE Samenhang met andere beleidsdocumenten

Het Alliander Privacy Beleid hangt samen met andere beleidsdocumenten die betrekking hebben op data en de protectie hiervan. Denk hierbij onder andere:

- Alliander Record Management Beleid
- Risicomanagement beleid
- Compliance beleid
- Alliander Kwaliteitsbeleid
- Informatiebeveiligingsbeleid
- Alliander Gedragscode: “Zo doen we dat bij Alliander”
- Alliander beleid ten aanzien van informatiedragers

Ook deze documenten kunnen geraadpleegd worden voor meer informatie betreffende bescherming van persoonsgegevens.