Alliander Tactisch Data- en Informatie Classificatiebeleid

Versie	1.0
Status	**Definitief**
Datum	06-02-2024
Opdrachtgever	Data Office
Projectleider	Product Owner G&S
Auteur(s)	Donné de Ruijter, Nicky Delclef
Reviewers	Mike Arends, Siema Manniesing, Rob Jansen, Mariëlla Son, Michiel Stoetzer, Marcel van der Wal, Maarten Venhoek, Raymond van Dijk
Classificatie	Intern

Versielog

Versielog	Datum	Auteur	Opmerking
0.1	8 november 2023	Nicky Delclef	Eerste conceptversie van beleidsdocument opgezet o.b.v. eerder opgestelde richtlijn
0.2	22 november ’23	Nicky Delclef en Donné de Ruijter	Feedback verwerkt van Privacy en Juridische Zaken stuk gedeeld voor review CISO
0.3	15 dec. 23	Donné de Ruijter	Opmerkingen Security verwerkt
0.7	19 dec 2023	Nicky Delclef	Document aangeboden ter slotreview aan stakeholders
0.9	26 jan. 24	Donné de Ruijter	Slotreview verwerkt. Beleid aangeboden aan MT Data Office ter accordering
1.0	6 feb. 24	Mt Data Office	Vastgesteld

Inhoud

1 Introductie

1.1 Achtergrond

Data Office speelt een belangrijke rol in het opstellen van beleid rondom Data en Informatie Management, Governance en Literacy (geletterdheid). Dit beleid is essentieel in het kader van de energietransitie, waarbij betrouwbare en goed beheerde data van groot belang is voor het realiseren van onze doelstellingen. Om de brug te slaan tussen het beleid en de daadwerkelijke uitvoering, heeft Data Office een Data en Informatie Classificatiebeleid opgesteld. Hierin wordt uiteengezet wat data en informatieclassificering inhoudt en hoe dit kan worden toegepast binnen de organisatie.

1.2 Drijfveren

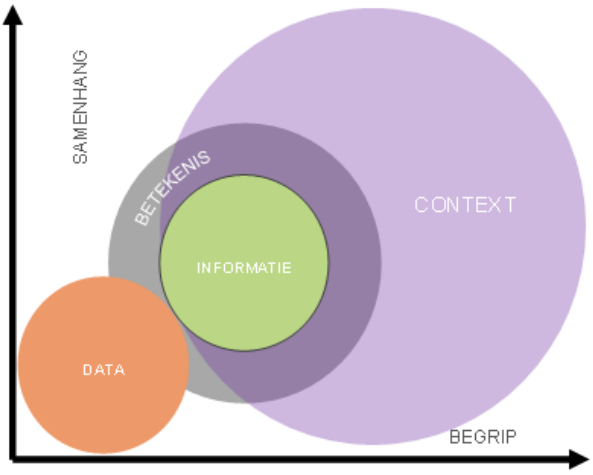
Om de waarde van data en informatie optimaal te benutten voor het versnellen van de energietransitie is het randvoorwaardelijk om data en informatie te classificeren. Classificaties zeggen iets over het te nemen beschermingsniveau, maar ook over de kwaliteit van data en informatie.

Want wat als de data en informatie waarmee je werkt (tijdelijk) niet beschikbaar is? Je bent bijvoorbeeld gehackt of je applicatie werkt niet meer door een systeemfout. Hoeveel dataverlies is dan geoorloofd voordat er problemen ontstaan? En wat als de data en informatie waarop je vertrouwt niet blijkt te kloppen? Worden er dan verkeerde beslissingen genomen? En zo ja, wat is dan de impact daarvan voor Alliander, haar klanten en medewerkers? En wat te doen als (bedrijf)vertrouwelijke informatie in verkeerde handen is gevallen? Of bij een datalek? Wat is de impact dan voor Alliander en betrokkenen?

De drijfveer achter dit beleid is te zorgen voor harmonisatie van classificatie en borging ervan in de gehele data- en informatieketen.

1.3 Data-Informatie-Kennis

In de wereld van data- en informatiemanagement maken we vaak een onderscheid tussen 'data' en 'informatie'. 'Data' verwijst naar de ruwe, onbewerkte feiten zonder directe betekenis, terwijl 'informatie' gezien wordt als data die waarde en betekenis heeft gekregen door een bepaalde context. Bij Liander zijn de metingen van onze netwerksensoren een voorbeeld van ruwe data.



Figuur 1: van data naar informatie

Echter, wanneer deze metingen worden aangevuld met relevante details zoals datum, tijd en locatie, veranderen ze van eenvoudige data naar bruikbare informatie. Waar in dit document wordt gerefereerd aan data en/of informatie dient daaronder te worden verstaan: ‘Alle data en informatie die Alliander maakt, bewaart en gebruikt, zowel in systemen (gestructureerd) als in documenten (ongestructureerd)’. Figuur 1 illustreert het verschil tussen data en informatie.

1.4 Doelstelling

Door het classificeren van data en informatie kunnen passende beheersmaatregelen gekozen worden om data en informatie te beschermen. Passend wil zeggen dat noodzakelijke maatregelen getroffen worden om risico’s te beheersen. Risicobeheersing is gericht op het voorkomen of beperken van schade. Denk hierbij aan imago- en reputatieschade, financiële schade, juridische schade, materiele- en immateriële schade. Dit beleid geeft regels om op een gestandaardiseerde manier data en informatie te classificeren. Het classificeren wordt gedaan op basis van *Beschikbaarheid, Integriteit, Vertrouwelijkheid*. In dit beleid wordt uitgelegd wat deze classificaties betekenen.

1.4 Scope

Dit beleid beschrijft welke classificaties en labels we onderkennen binnen Alliander, en wat ze betekenen. Het beleid heeft betrekking op zowel ongestructureerde data en informatie (denk aan documenten, foto’s en tekeningen) als gestructureerde data en informatie (database met klantgegevens bijv.).

Dit beleid geldt voor iedere medewerker binnen Alliander exclusief new business[1]. Dit beleid geldt ook voor leveranciers, klanten, en overige derden waarmee data en informatie gedeeld wordt. Het *toepassen* van classificaties staat verder beschreven in de daarvoor bestemde (operationele) beleidsstukken.

Bij het toepassen van dataclassificaties speelt wetgeving bijvoorbeeld een rol. In veel gevallen mogen data en informatie, in bijzonder binnen het gereguleerde domein, niet zomaar aan iedereen binnen Alliander verstrekt worden, zoals bijvoorbeeld op basis van artikel 79 lid 1 Elektriciteitswet 1998 en artikel 37 lid 1 Gaswet. Deze artikelen verplichten de netbeheerder (Liander) tot geheimhouding van vertrouwelijke gegevens die de netbeheerder door zijn taakuitoefening heeft verkregen, tenzij de wet anders voorschrijft. Anderzijds moet data soms juist openbaar gemaakt worden, bijvoorbeeld om een gelijk speelveld te creëren voor bedrijven (artikel 79 lid 2 Elektriciteitswet 1998). Dat laatste doet Alliander niet alleen vanuit een wettelijke taak maar ook om actief innovatie te stimuleren.[2]

1.5 Gerefereerde documenten

- Alliander Data en Informatie Governance Beleid.pdf.[3]
- Alliander Privacy Beleid[4]
- Strategisch Alliander Security Beleid[5]
- ISMSVI-A05-K-03-Beleid voor Geclassificeerde Informatie v2023-04.pdf[6]:
- ISO/IEC 27001:2013 norm, A.8.2.1; A.8.2.2; A.8.2.3; A.8.3.1; A.8.3.3; A.9.4.1; A.13.2.3
- ISO/IEC 27001:2022 norm, A5.10; A5.12; A5.13; A5.14; A7.10; A8.3
- ISO/IEC 27001:2017 maatregelenset, A6.1.7; A12.9.1

1.6 Geldigheid en documentbeheer

Dit document is geldig vanaf 6 februari 2024. De eigenaar van dit document is Data Office. Data Office is regiehouder en dient het document minstens één keer per jaar te controleren – indien nodig bij te werken – en op te slaan onder een nieuw versienummer. Bij wijzigingen van dit document dient het document opnieuw goedgekeurd te worden.

[1] Onze organisatie - Alliander

[2] Data delen vormt een van de zeven strategische pijlers van Alliander: Meer inzicht - dankzij data als strategische asset! : Intranet (alliander.com).

[3] Heeft als doel om duidelijke processen, kaders, regels en richtlijnen voor te schrijven, voor de wijze waarop Alliander haar data en informatie verwerkt, levert en diensten verricht.

[4] Heeft als doel om duidelijke processen, kaders, regels en richtlijnen voor te schrijven, voor de wijze waarop Alliander met persoonsgegevens dient om te gaan Informatie gebruiken : Intranet (alliander.com).

[5] Securitybeleid : Intranet (alliander.com) beschrijft hoe security is ingericht en wordt bestuurd binnen Alliander. https://intranet.alliander.com/risico-management beschrijven de maatregelen die minimaal genomen moeten worden op basis van een BIV-score.

[6] Is het leidende beleidsdocument voor het toepassen van classificaties op data die behoort tot de vitale infrastructuur. Zie voor deze en andere beleidsstukken: Asset- en Productmgt publicaties (Alliander excl. New Business) - SOVI Beleid - Alle documenten (sharepoint.com).

2. Beschikbaarheid, Integriteit en Vertrouwelijkheid

2.1 Definities

Een BIV-classificatie is een indeling die wordt gebruikt om de Beschikbaarheid (continuïteit), de Integriteit (betrouwbaarheid) en de Vertrouwelijkheid (exclusiviteit) van data en informatie aan te geven.

Beschikbaarheid gaat over de mate waarin data en informatie nodig is om de bedrijfscontinuïteit te garanderen. Dit wordt afgewogen tegen de risico's wanneer data en informatie niet beschikbaar is. De consequenties hiervan variëren van lichte irritaties of ongemak bij medewerkers - omdat bijvoorbeeld de toegang tot een systeem tijdelijk is uitgevallen en daardoor (tijdelijk) het werk niet kan worden gedaan - tot financiële en juridische schade door het niet kunnen leveren van diensten aan de klant (contractuele en wettelijke verplichtingen).

Integriteit gaat over de mate waarin de data en informatie juist, valide en betrouwbaar is. Ook dit wordt afgewogen tegen de risico's. De consequenties hiervan hangen af van de aard en context waarin de beslissing genomen wordt. Een verkeerd gespelde naam (aanhef) in een mail heeft weinig consequenties zolang de geadresseerde maar klopt. De geadresseerde zal snappen dat het om een typefout gaat. Maar wordt er bijvoorbeeld een gasleiding geraakt met graafwerkzaamheden op basis van onjuiste gegevens waardoor er veiligheidsrisico's optreden, dan is de impact groot.

Vertrouwelijkheid gaat over de mate waarin data en informatie openbaar gemaakt mag worden. Dat wordt vastgesteld met bevoegdheden en de mogelijkheden tot muteren, kopiëren, toevoegen, vernietigen of kennisnemen van data en informatie voor een gedefinieerde groep van gerechtigden. Ongeautoriseerde toegang tot bedrijfsgevoelige- of persoonsgegevens kan o.a. leiden tot imago- en reputatieschade voor het bedrijf, en verlies van vertrouwen door klanten en medewerkers. Verder kan dit een schending van wet- en regelgeving betekenen.

2.2 Classificatiemodel

Het BIV-classificatiemodel (zie tabel 1, 2 en 3) kent 5 verschillende niveaus, labels en bijbehorende classificatiecriteria. Niveau 1 impliceert weinig risico en een lage impact voor de beschikbaarheid, integriteit en vertrouwelijkheid van data en informatie, terwijl niveau 5 een hoge impact impliceert. Het niveau bepaalt de minimale set aan maatregelen die genomen moeten worden om risico's te mitigeren. De te nemen maatregelen bij een betreffende BIV-score zijn te vinden in BIA_template_v2.xlsm.

Tabel 1: Beschikbaarheid

Beschikbaarheid		
Niveau	***Label***	***Classificatie met criteria***
5	Zeer Hoog	Indien de data of informatie niet beschikbaar is, loopt Alliander zeer grote schade op.
4	Hoog	Indien de data of informatie niet beschikbaar is, loopt Alliander grote schade op.
3	Medium	Indien de data of informatie niet beschikbaar is, loopt Alliander gemiddelde schade op.
2	Laag	Indien de data of informatie niet beschikbaar is, loopt Alliander slechts geringe schade op.
1	Zeer Laag	Indien de data of informatie niet beschikbaar is, loopt Alliander geen schade op.

Tabel 2: Integriteit

Integriteit			
Niveau	***Label***	***Classificatie met criteria***	***Maatregel***
5	Zeer Hoog	Indien de data of informatie onjuist, onvolledig of niet tijdig is, loopt Alliander zeer grote schade op. Honderd procent	Automatische identificatie en onmiddellijke correctie

		juistheid/volledigheid van de gegevens is een eis.	
4	Hoog	Indien de data of informatie onjuist, onvolledig of niet tijdig is, loopt Alliander grote schade op. Incidenteel onjuistheden/onvolledigheden in de gegevens zijn acceptabel.	Automatische identificatie en onmiddellijke correctie
3	Medium	Indien de data of informatie onjuist, onvolledig of niet tijdig is, loopt Alliander onwenselijke schade op.	Automatische identificatie en correctie achteraf
2	Laag	Onjuiste, onvolledige of niet tijdige data en informatie leidt tot geringe schade. Beperkte absolute en lagere eisen aan de juistheid/volledigheid van de gegevens.	Identificatie en correctie achteraf
1	Zeer Laag	Onjuiste, onvolledige of niet tijdige data en informatie leidt niet tot schade. Geen eisen aan de juistheid/volledigheid van de gegevens.	Identificatie en correctie achteraf

Tabel 3: Vertrouwelijkheid

Vertrouwelijkheid			
Niveau	***Label***	***Classificatie met criteria***	***Toegangsbeperking***
5	Zeer Vertrouwelijk[7]	Informatie welke beschouwd moet worden als 'geheim' mag enkel gedeeld worden met anderen onder strikt vastgestelde voorwaarden welke goedgekeurd zijn door de Security Officer. En anders mogen deze niet gedeeld worden.	Alleen individuele toegang op basis van need-to-know[8] (intern en/of extern).
4	Vertrouwelijk[9]	Informatie die enkel gedeeld mag worden met individuele personen op 'Need-to-know' basis. Kennisname van deze informatie door hiertoe niet gerechtigde personen kan leiden tot ernstige financiële en/of imago schade aan de organisatie.	Alleen individuele toegang op basis van need-to-know (intern en/of extern) Extern delen alleen met NDA[10] indien relevant aangevuld met een verwerkingsovereenkomst.
3	Intern Beperkt	Informatie bedoeld voor intern gebruik die gedeeld mag worden binnen een afdeling of team werkend voor Alliander. Kennisname van deze informatie door hiertoe niet gerechtigde personen kan leiden tot financiële en/of imago schade aan (delen van) de organisatie.	Intern voor een (deel) afdeling van Alliander. (Inhuur en derden enkel met een getekende NDA)
2	Intern	Informatie bedoeld voor intern gebruik door alle medewerkers werkend voor Alliander. Kennisname van deze informatie door hiertoe niet gerechtigde personen kan leiden tot mogelijk financiële en/of imago schade aan (delen van) de organisatie.	Intern voor iedere Alliander medewerker, inhuur en derden met NDA
1	Publiek	Informatie bedoeld voor publicatie. Kennisname van deze categorie informatie brengt de organisatie geen enkele schade toe.	Alle informatie die publiekelijk beschikbaar is, kent geen vertrouwelijkheidsniveau maar dient wel integer te zijn.

[7] Zeer vertrouwelijk in deze kan ook gelezen worden als 'Geheim' en dient dan ook als een geheim behandeld te worden

[8] Need to know' beschrijft het principe dat de toegang tot een informatie die als gevoelig beschouwd wordt, strikt beperkt wordt tot die personen die hem nodig hebben.

[9] Voor Persoons herleidbare (PII) gegevens dienen de classificatie richtlijnen vanuit Alliander Privacy gevolgd te worden.

[10] Staat voor Non Disclosure Agreement: Digitaal Geheugen - NDA documenten - Alle documenten (sharepoint.com)

3. Criteria voor classificatie documenten

Om het beschermingsniveau te bepalen is het belangrijk om de waarde van data en informatie in een document te bepalen, waarbij geldt dat de meest vertrouwelijke data en informatie in een document, het beschermingsniveau dient te bepalen. Om hier invulling aan te geven is het belangrijk dat een documenteigenaar op een document meegeeft hoe belangrijk de data en informatie in het document voor de documenteigenaar is, en hoe de data en informatie daarna verder behandeld dient te worden. Zie bijlage 3 voor een praktische handreiking hoe om te gaan met documenten. Het opvolgen van onderstaande beleidskeuzes ondersteunt daarmee het borgen van het veilig houden van de waardevolle data en informatie en dient dan ook opgevolgd te worden.

Documenten die niet gelabeld zijn, mogen niet vrijblijvend gedeeld of bewerkt worden. Hierbij moet het document behandeld worden als zijnde geclassificeerd. Informeer bij de documenteigenaar, bij de verantwoordelijke manager of bij een Security Manager bij twijfel over hoe het document behandeld moet worden.

3.1 Stappen en verantwoordelijkheden

Stappen en verantwoordelijkheden voor informatiebeheer zijn:

Naam stap	*Verantwoordelijkheid*
1. Classificatie van data en informatie	Eigenaar van document/ informatie
2. Labelen data en informatie 2. Classificeren en labelen van extern verkregen informatie	Eigenaar van document/ informatie Ontvanger/ geadresseerde van document
3. Behandeling data en informatie	Personen met toegangsrechten in overeenstemming met dit Beleid

Indien data en informatie wordt ontvangen van buiten de organisatie, dan is de ontvanger verantwoordelijk voor de classificatie ervan in overeenstemming met de regels voorgeschreven in dit beleid. Deze persoon wordt eigenaar van een dergelijk document. Tenzij er al een andere eigenaar in de organisatie bestaat van deze data of informatie.

3.2 Criteria voor classificatie

De classificatie (niveau van vertrouwelijkheid) wordt bepaald aan de hand van de volgende criteria[11]:

- Waarde van data en informatie gebaseerd op de classificatiecriteria;
- Gevoeligheid en kritiek zijn van data en informatie gebaseerd op het hoogst berekende risico voor elk item van data en informatie gebaseerd op de classificatiecriteria;
- Persoonlijke risico's voor medewerkers;
- Wetgeving en contractuele verplichtingen gebaseerd op de lijst wet-, regelgeving en contractuele verplichtingen;
- Data en informatie die vanuit de primaire dienstverlening als vertrouwelijk behandeld dient te worden om misbruik en reputatieschade te voorkomen;
- Diensten (Gas- & Elektriciteitsvoorziening) en data en informatie vanuit leveranciers welke als kritisch en of vertrouwelijk beschouwd moet worden om te voorkomen dat Alliander als onbetrouwbare partner gezien wordt en reputatieschade lijdt.
- De basisregel is het laagste niveau van vertrouwelijkheid te gebruiken die nog een geschikt niveau van beveiliging waarborgt, om zo onnodige beveiligingskosten te voorkomen.

3.3 Labelen van informatie

Classificatieniveaus van vertrouwelijkheid worden op de volgende manier gelabeld:

- **Papieren documenten** de classificatie wordt aan de onderkant van elke pagina aangegeven in de vorm van een classificatielabel; het label wordt eveneens aangegeven op de voorkant van het schutblad of envelop met als inhoud een dergelijk document alsook de archiefmap waarin het document wordt opgeslagen.
- **Elektronische documenten** de classificatielabel wordt aangegeven aan de onderkant van elke pagina in het document. Daarnaast ook op de titelpagina.
- **Elektronische mail** het classificatieniveau van vertrouwelijke en zeer vertrouwelijke geclassificeerde informatie in een e-mail wordt aangegeven in de eerste regel van de e-mail hoofdtekst.

[11] Zie in bijlage 2 een beslisboom voor de praktische vertaling van criteria naar labels

- **Mondeling overgebrachte informatie** de classificatie van de vertrouwelijke informatie die van mond tot mond, telefonisch of met andere verbale middelen wordt overgebracht – voor zover het niet als publiek geclassificeerde informatie betreft – dient voorafgaand aan de informatie te worden aangegeven.

In situaties waarbij data en informatie niet gelabeld kan of mag worden i.v.m. aantasting van de integriteit en of technische beperkingen, dan dient deze data of informatie behandeld te worden alsof deze geclassificeerd is, en bij voorkeur daar opgeslagen te worden waar vergelijkbare maatregelen getroffen zijn; passend bij de classificatie.

3.4 Lijst van geautoriseerde personen

Data en informatie geclassificeerd als "Vertrouwelijk" dient vergezeld te gaan met een Lijst van Geautoriseerde Personen waarin de documenteigenaar de namen specificeert of functies of personen die toegangsrechten mogen hebben op die data of informatie. Dezelfde regels gelden voor het niveau van vertrouwelijkheid “Intern beperkt” indien mensen buiten de organisatie toegang hebben tot een dergelijk document.

3.5 Herclassificatie

Documenteigenaren moeten het niveau van vertrouwelijkheid van hun informatiebedrijfsmiddelen periodiek herbeoordelen of het niveau van vertrouwelijkheid kan worden gewijzigd. Indien mogelijk dient het niveau van vertrouwelijkheid te worden aangepast.

4. Classificeren van Gestructureerde Data

Eenduidige registratie van data is noodzakelijk voor Alliander. De informatiebehoefte is vastgelegd per basisregistratie middels een informatiemodel. In dit model staat de informatiebehoefte van Alliander t.a.v. de basisregistratie, inclusief de bijbehorende definities. Een basisregistratie is een noodzakelijk register waarin gegevens zijn opgenomen[12]. Een consument van data moet voor zijn taakuitoefening gegevens uit de daarvoor bestemde basisregistratie gebruiken. Om die reden classificeren we gestructureerde data in het informatiemodel die ten grondslag ligt aan de basisregistratie.

Een basisregistratie kent doorgaans meerdere registers. Een register is een gestructureerde en gecontroleerde verzameling van data die informatie bevat over een bepaald onderwerp binnen een basisregistratie. Een register is als de centrale bron voor dat onderwerp. De gegevens van dat onderwerp worden gestandaardiseerd en gevalideerd volgens vastgestelde regels. Registers kunnen bijvoorbeeld worden gebruikt om bepaalde klantgegevens bij te houden. Ze zorgen voor consistentie en nauwkeurigheid van de informatie en zijn de basis voor de hele organisatie die deze gegevens consumeert.

De feitelijke toekenning van classificaties vindt plaats in het onderliggende informatiemodel van een basisregistratie. De verantwoordelijkheid voor de totstandkoming van het informatiemodel berust bij de betreffende datadomeinmanager[13].

Het doel van het classificeren van data in het informatiemodel is het toekennen van waarde aan data. De centrale vraag wordt beantwoord: *In welke mate moét deze data beschikbaar, integer en vertrouwelijk zijn?* Dit in tegenstelling tot het classificeren van dataproducten waarin een Verstrekker aan potentiële dataconsumenten (afnemers) aangeeft *welke mate van beschikbaarheid, integriteit gegarandeerd wordt en welke vertrouwelijkheidsniveau op het dataproduct van toepassing is* op moment van verstrekking. Het classificeren van dataproducten wordt nader beschreven in operationeel beleid.

4.1 Criteria voor classificeren van gestructureerde data

Classificaties kunnen op verschillende niveaus worden toegepast. Uitgangspunt is om op een zo hoog mogelijk niveau te classificeren. Daarvoor dient eerst naar de onderliggende attributen gekeken te worden:

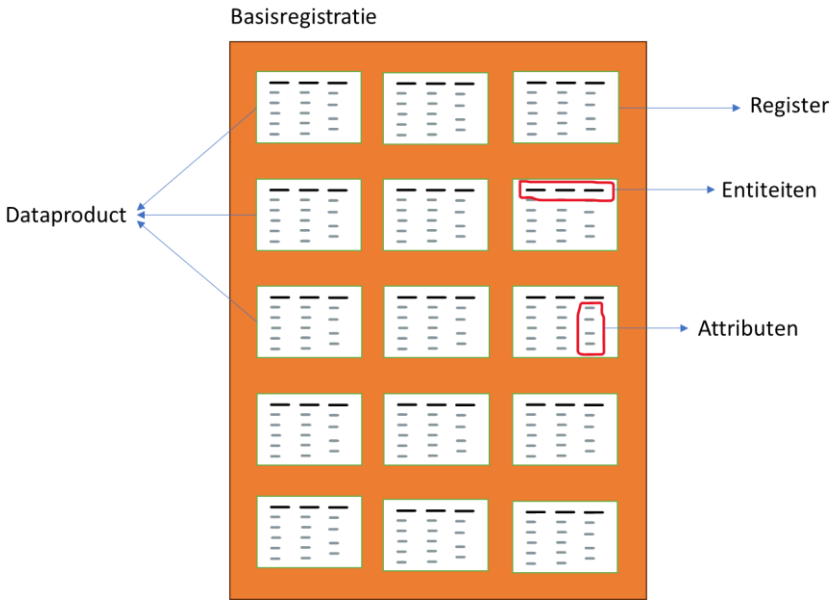
- In basis wordt er op attribuutniveau geclassificeerd. Een attribuut is een beschrijvende

[12] Alle basisregistraties met de daarin behorende registers en verantwoordelijkheden zijn te raadplegen via: Basisregistratie - Data Office - Confluence (atlassian.net).

[13] Functie binnen het Data Office die gesprekspartner is voor de opdrachtgever en rentmeester. De datadomeinmanager vormt de brug tussen het beleid en kaders van het centrale Data Office en de business behoefte van de bedrijfsonderdelen.

eigenschap van een entiteit. De attributen ‘voornaam’ en ‘achternaam’ zeggen bijvoorbeeld iets over de entiteit ‘klant’.

- Indien de classificatie van alle attributen van een entiteit gelijk is, dan kan er op entiteitniveau geclassificeerd worden. Een entiteit is iets waarover we informatie verzamelen. Denk bijvoorbeeld aan een ‘klant’ of ‘kabel’.
- Indien de classificatie van alle entiteiten binnen een register gelijk zijn dan kan er op registerniveau geclassificeerd worden. Een register is een gestructureerde en gecontroleerde verzameling van data die informatie bevat over een bepaald onderwerp binnen een basisregistratie. Voorbeelden zijn het Meetwaardenregister, het Klantregister en het Werkactiviteit register.



Figuur 2: registerdata

Zoals figuur 3 laat zien vormt een set van attributen een entiteit, een aantal entiteiten een register en een aantal registers een basisregistratie.

4.2 Stappen en Verantwoordelijkheden

De eindverantwoordelijkheid dat alle data in een basisregistratie geclassificeerd is berust bij de betreffende Opdrachtgever. De Data Rentmeester is als beheerder van een of meerdere registers binnen een basisregistratie eindverantwoordelijk voor het classificeren van data en informatie. De Data Rentmeester benoemt een of meerdere Data Stewards die (o.a.) de uitvoerende verantwoordelijkheid hebben om de data en informatie in het informatiemodel feitelijk te classificeren. Data Stewards kunnen een Privacy Officer, Security Manager en eventueel andere domeinexperts consulteren.

	R	A	S	C	I[14]
Opdrachtgever		X			
Data Rentmeester		X			
Data Steward	X				
Security Manager				X	
Privacy Officer				X	

Tabel 4: RASCI-tabel voor dataclassificatie informatiemodel

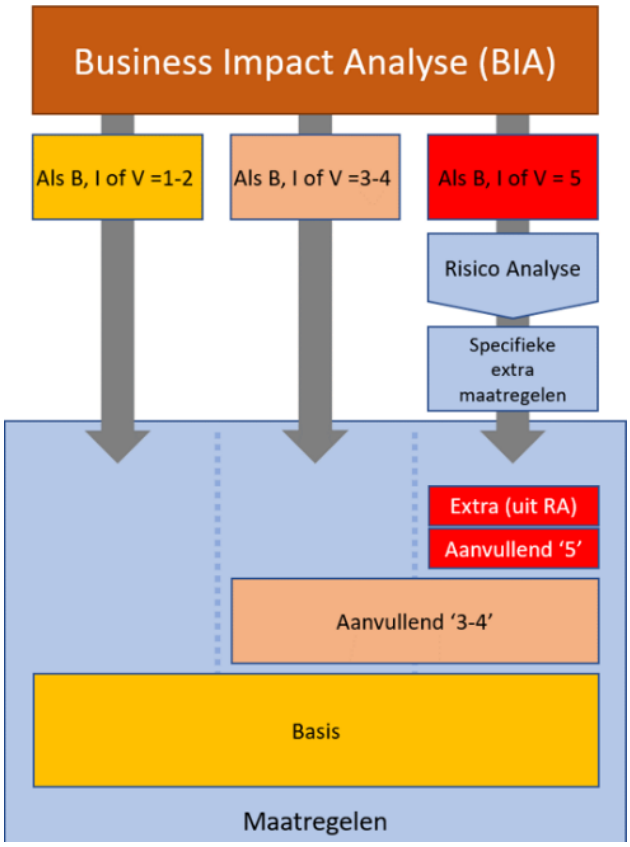
Zie voor een definitie en omschrijving van deze en andere governancerollen, het Alliander Data en Informatie Governance Beleid.pdf.

[14] RASCI staat voor Responsible, Accountable, Supportive, Consulted en Informed. Hiermee wordt de verantwoordelijkheidsverdeling middels een kruisje duidelijk gemaakt.

Data en informatie die beheerd wordt in registers komen voort uit processen. Processen maken het doel duidelijk waarvoor - en de context waarin - gegevens geregistreerd en gebruikt worden. Processen worden getoetst aan de hand van een Business Impact Assessment (BIA)[15]. Het resultaat van een BIA leidt tot een BIV-score en te nemen maatregelen zoals ook te zien in figuur 3.

Er is niet altijd een 1-op-1-relatie tussen processen en data die in registers wordt beheerd. Wel kunnen BIA's een belangrijke bron van informatie zijn om attributen, entiteiten te classificeren. Data Stewards kunnen daarom de volgende stappen nemen om data en informatie in het informatiemodel te classificeren:

- Vaststellen van de onderliggende (kritieke) processen;
- Inventariseren en onderzoeken van (BIA's) die daarop uitgevoerd zijn en adviseren tot het uitvoeren van ontbrekende BIA's;
- Alle relevante BIV-classificaties verzamelen afkomstig uit de BIA's en toepassen op de relevante attributen, entiteiten. Data Stewards kunnen hulp en ondersteuning inschakelen van een Privacy Officer, Security Manager en andere domeinexperts.



De kleur van de BIV-score heeft dezelfde kleur als de set van maatregelen die daarvoor gelden. Zo geldt bijvoorbeeld de maatregelen set 'Basis' voor data en informatie met een BIV-score 1-2. Een BIV-score van 5 wil zeggen dat de maatregelen set 'Basis' en 'Aanvullend' gelden, alsmede een aanvullende risico-assessment.

De verantwoordelijkheden voor het classificeren van gegevens die buiten een basisregistratie worden vastgelegd en beheerd, vallen buiten scope van de governance zoals bedoelt in tabel 4. In plaats daarvan gelden de twee basisuitgangspunten conform het Alliander Data en Informatie Governance Beleid.pdf:

1. Dat wat je maakt aan data en informatie ben je verantwoordelijk voor;
2. Dat wat je ontvangt aan data en informatie mag je eisen aan stellen.

De verantwoordelijkheid voor het classificeren van data en informatie die buiten een basisregistratie wordt beheerd, berust dus bij de maker. Wel dienen dezelfde classificatielabels gehanteerd te worden zoals beschreven in dit beleid, alsmede de daarmee samenhangende te nemen maatregelen.

Figuur 3: BIV-score en maatregelen

4.3 Herclassificatie

Iedere wijziging in het conceptuele informatiemodel die ten grondslag ligt aan een basisregistratie noodzaakt een herclassificatie. Het kan bijvoorbeeld gaan om een veld dat wordt toegevoegd, verwijderd of gewijzigd in het informatiemodel. Of nieuwe of gewijzigde wet- en regelgeving die nieuwe eisen stellen aan het classificeren van data. Minimaal wordt er jaarlijks een controle uitgevoerd op de juistheid en actualiteit van dataclassificaties in het informatiemodel. Hiervoor is de Opdrachtgever eindverantwoordelijk en Data Stewards uitvoerend verantwoordelijk.

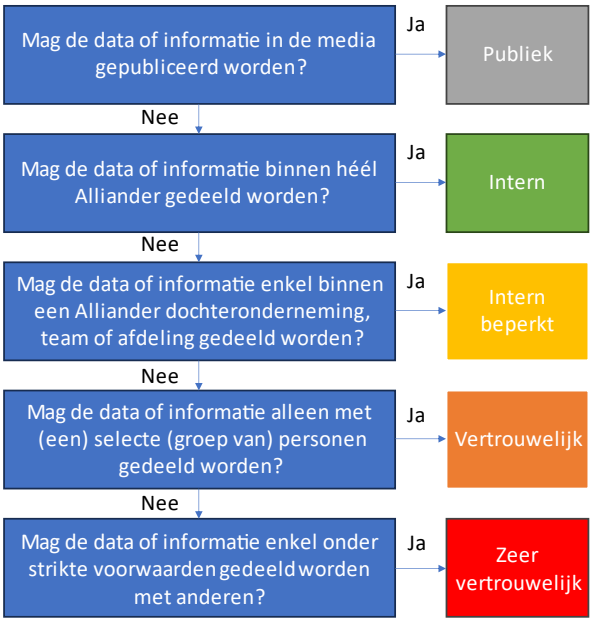
[15] De BIA heeft tot doel om o.a. de financiële, operationele, klant- en medewerker gerelateerde gevolgen te bepalen van het bedrijfsproces of onderliggend systeem: BIA_template_v2.xlsm.

Bijlage 1: Begrippenlijst

Begrip	Definitie	Voorbeeld
Beschikbaarheid, Integriteit, Vertrouwelijkheid (BIV)	Classificatiemethode om aan te geven in welke mate data en informatie beschikbaar, integer en vertrouwelijk moet zijn.	Beschikbaarheid: we kunnen bij de gegevens op het moment dat dat nodig is. Integriteit: de gegevens zijn juist, betrouwbaar en valide. Vertrouwelijkheid: de (persoons)gegevens zijn passend afgeschermd.
Data	Ongefilterde, niet-geïnterpreteerde data (ruwe gegevens)	Zoals data uit slimme meters en laadpalen.
Data-Informatie-Kennis-Wijsheid Model	De notie dat hiërarchisch gezien Wijsheid (kennis in een raamwerk meervoudig toepasbaar) zich ontwikkelt vanuit Kennis (het verklaren van hoe en waarom). Kennis wordt gevoed door Informatie (gerelateerde data binnen een context) wat voortkomt uit technisch vastlegging van ruwe gegevens (Data).	
Data Governance	Het implementeren en handhaven van autoriteit en controle over het beheer van data, inclusief alle bijbehorende middelen zoals het geheel van beleidsregels, beheersmaatregelen, afspraken processen en procedures die bepalen door wie, hoe en waarom data gebruikt wordt. Eenduidig belegde rollen maken duidelijke sturing van de informatiehuishouding van Alliander mogelijk.	
Data Lifecycle Management	Het proces van het beheren van data vanaf creatie, gebruik en veroudering tot verwijdering. Data Lifecycle Management is cruciaal om middelen effectief te kunnen gebruiken en te voldoen aan regelgeving.	
Databeveiligingsmanagement	Betreft de processen, procedures beleidsregels, technologieën om de beschikbaarheid, integriteit en vertrouwelijkheid van de data te waarborgen.	
Datamanagement	Betreft de processen, procedures, beleidsregels, technologieën en architectuur om data te beheren gedurende de hele levenscyclus, waaronder definiëren, transformeren, besturen, kwalitatief bewaken, beveiligen, beschikbaar stellen en vernietigen.	
Document & Contentmanagement	Beheert de lifecycle van data en informatie in ongestructureerde vorm.	Voorbeelden van documenten zijn o.a. policies, regelgevingen, handleidingen en werkinstructies.

Gestructureerde Data	Gegevens die zich conformeren aan een bepaald patroon.	Kenmerken vastgelegd in de HR-database, zoals naam, adres, woonplaats, functie, afdeling en personeelsnummer.
Informatiemodel	Model(lering) van de werkelijkheid binnen het beschouwde domein, v.w.b. informatie daarvan, en is onafhankelijk van ontwerp van en implementatie in systemen. Het geeft een zo getrouw mogelijke beschrijving van die werkelijkheid en is in natuurlijke taal geformuleerd. Een dergelijk model definieert het ‘wat’: welke ‘concepten’ (‘dingen’) worden onderscheiden (in de beschouwde werkelijkheid), wat betekenen zij, hoe verhouden ze zich tot elkaar en welke informatie (eigenschappen) is daarvan relevant.	
Metadata	Beheert de “data over de data”. Metadata registreert gebeurtenissen (wie heeft wat op welk moment en waar gemuteerd) en labelt de data. Ze is essentieel voor een beter beheer en gebruik	Datum en tijdstip van aanmaak, versies, logging, BIV-classificatie, labels, data herkomst.
Metadatamanagement	Het beheer van gegevens over gegevens.	
Ongestructureerde Data	Gegevens die zich niet conformeren aan een bepaald patroon.	Documenten (Word en PDF), foto’s, tekeningen en video’s

Bijlage 2: Beslisboom Vertrouwelijkheid



Bijlage 3: Omgaan met data en informatie

	Publieke informatie	Interne en Intern beperkte informatie	Vertrouwelijke informatie	Zeer vertrouwelijke informatie
Fysieke post	Open enveloppe of folder.	Gesloten enveloppen geadresseerd aan de beoogde ontvanger.	Gesloten enveloppe persoonlijk geadresseerd aan de need-to-know ontvanger.	Informatie wordt persoonlijk of door een koerier overhandigd
Opbergen	Openbare informatie hoeft niet te worden opgeborgen.	Opbergen in een af te sluiten kast of lade, waar alleen medewerkers toegang toe hebben.	Opbergen in een af te sluiten kast of lade waar alleen need-to-know medewerkers toegang toe hebben.	Opbergen in een af te sluiten kast of lade waar alleen need-to-know medewerkers toegang toe hebben.
Weggooien	De informatie mag in iedere papiercontainer worden weggegooid.	Gooi het papier in de blauwe papierbak voor vertrouwelijke informatie die je bij de printers kan vinden.	Gooi het papier in de blauwe papierbak voor vertrouwelijke informatie bij de printers.	Gooi het papier in de blauwe papierbak voor vertrouwelijke informatie bij de printers.
Copy/Print/ Scan	De informatie mag op iedere multifunctionele printer worden geprint, gescand of gekopieerd.	Gebruik de interne Alliander printer via follow me printer. Of print het via een leverancier of partner waarmee we geheimhouding of een verwerkersovereenkomst hebben afgesproken.	Via follow me printen en blijf bij de printer tot het gereed is. Of print het via een leverancier of partner waarmee we geheimhouding of een verwerkers-overeenkomst hebben afgesproken.	Alleen kopiëren, printen en scannen na toestemming van de document eigenaar. Via follow me printen en blijf bij de printer tot het gereed is.
Conference Call	Gebruik een willekeurige telefoon of ander device om openbare informatie te bespreken.	Gebruik alleen Alliander telefoons en devices voor het voeren van interne gesprekken. Gebruik MS Teams. Zorg ervoor dat gesprekken niet kunnen worden meegeluisterd door onbevoegden.	Gebruik alleen Alliander telefoons en devices voor het voeren van vertrouwelijke gesprekken, MS Teams. Zorg ervoor dat gesprekken niet kunnen worden meegeluisterd door onbevoegden.	Gebruik alleen Alliander telefoons en devices voor het voeren van vertrouwelijke gesprekken, MS Teams. Zorg ervoor dat gesprekken niet kunnen worden meegeluisterd door onbevoegden
Verwerken informatie	Je mag openbare informatie overal op verwerken. Publiceren namens Alliander mag alleen na goedkeuring van de afdeling marketing.	Interne informatie mag alleen worden verwerkt op een Alliander device of op een BYOD binnen de Alliander Citrix omgeving. Informatie moet in de juiste mappen of systemen worden opgeslagen waartoe alleen medewerkers toegang hebben.	Vertrouwelijke informatie mag alleen worden verwerkt op een Alliander device of een BYOD binnen de Alliander Citrix omgeving. Vertrouwelijke informatie moet in de map '00 Vertrouwelijk' worden opgeslagen op de CS of in een Teams/SharePoint map met vertrouwelijk karakter.	Zeer Vertrouwelijke informatie mag alleen worden verwerkt op een Alliander device of een BYOD binnen de Alliander Citrix omgeving. Vertrouwelijke informatie moet in de map '00 Vertrouwelijk' worden opgeslagen op de CS of in een Teams/SharePoint map met vertrouwelijk karakter
Opslaan op mobiel medium	Openbare informatie mag op een USB stick of ander opslagmedium worden opgeslagen.	Interne informatie mag alleen vercijferd worden opgeslagen op een USB stick of ander opslagmedium.	Vertrouwelijke informatie mag alleen vercijferd worden opgeslagen op een USB stick of ander opslagmedium.	Zeer vertrouwelijke informatie mag niet op externe gegevensdragers worden opgeslagen
Email en agenda-items	Openbare informatie mag onvercijferd naar ontvangers	Interne informatie mag onvercijferd binnen Alliander en Qirion worden verstuurd, maar alleen naar ontvangers die de informatie mogen inzien.	Vertrouwelijke informatie mag onvercijferd binnen Alliander en Qirion worden verstuurd, maar alleen naar ontvangers die de informatie mogen inzien.	Zeer vertrouwelijke informatie mag alleen intern via e-mail/Teams gedeeld worden en uitsluitend met toestemming van de eigenaar

16

[16] Bron: Qirion - Onepager_Omgaan met informatie.pdf - Alle documenten (sharepoint.com)