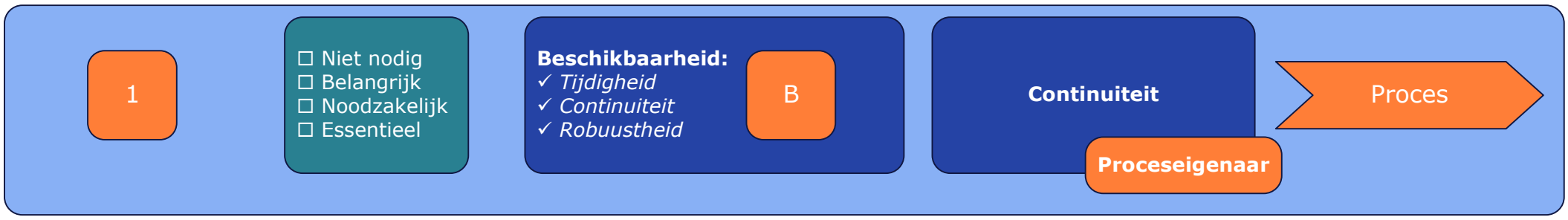
Denkkaders kwaliteitscriteria

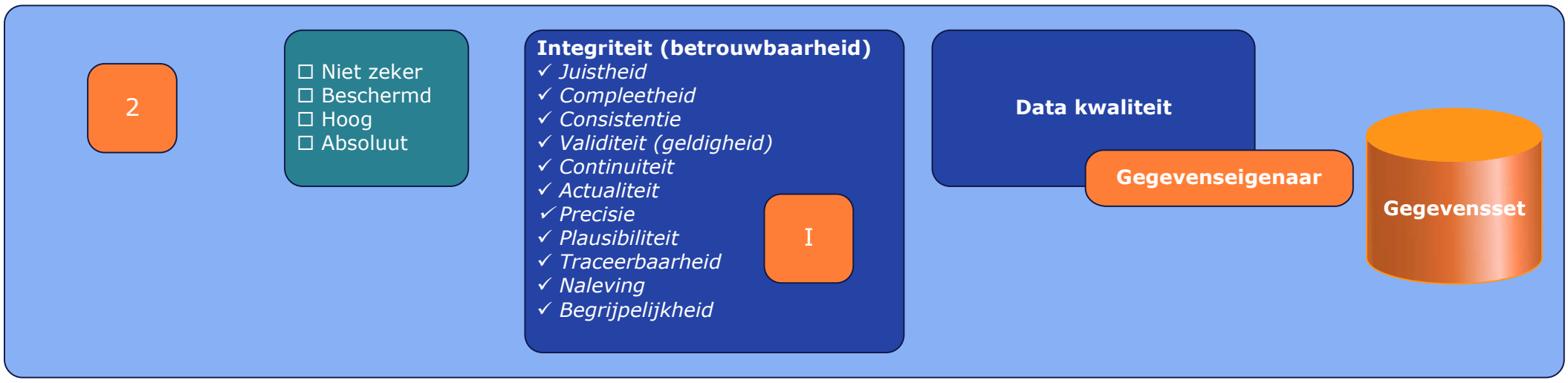
Kwaliteitscriteria

Als gegevens een onmisbare pijler zijn van onze informatievoorziening en van onze beslissingsondersteuning is de kwaliteit van die gegevens in hoge mate bepalend voor de kwaliteit van onze informatie en van onze beslissingen. Het begrip 'gegevenskwaliteit' kan worden gedefinieerd als de mate waarin de karakteristieken van de gegevens voldoen aan expliciete en impliciete behoeften onder gespecificeerde condities. Of populair uitgedrukt: 'fit for use', een omschrijving die duidelijk maakt dat de afnemer bepaalt wat de gewenste kwaliteit is.

Inzichtelijk maken van datakwaliteit binnen de gemeente Oss

Datakwaliteit zegt iets over de Beschikbaarheid, Integriteit en Vertrouwelijkheid van de data. De zogeheten BIV-classificatie.





Goed datamanagement ten aanzien van continuïteit, kwaliteit en vertrouwelijkheid begint met een goede BIV-classificatie (**B**etrouwbaarheid, **I**ntegriteit, **V**eiligheid). Om de BIV-classificatie inzichtelijk te krijgen en de datakwaliteit binnen de gemeente Oss te organiseren moet per proces bepaald worden:

1 **Stap 1:** Hoe bedrijfkritisch is het proces?
Met andere woorden: wat betekent het voor de gemeente Oss of afnemers wanneer dit proces tijdelijk uitvalt?
Welke risico's loopt de organisatie dan?

2 **Stap 2:** Hoe betrouwbaar moet de data zijn als output van het proces?
Met andere woorden: hoe bedrijfkritisch is de data voor onze organisatie?

3 **Stap 3:** Aan welke mate van vertrouwelijkheid moet de data voldoen?
Met andere woorden: welke data mag onze gemeente delen, hoe lang mag onze gemeentelijke data bewaren, welke data mag bewaard worden en wie mag deze data inzien?

Toelichting beschikbaarheid

Beschikbaarheid:
✓ *Tijdigheid*
✓ *Continuiteit*
✓ *Robuustheid*

Tijdigheid

Tijdigheid bij de beschikbaarheid van data binnen een proces verwijst naar het vermogen om de benodigde data op het juiste moment beschikbaar te hebben, zodat het proces efficiënt en effectief kan verlopen. Dit betekent dat de data op een zodanig tijdstip beschikbaar is dat het de beslissingen, acties of operaties binnen het proces optimaal ondersteunt. Het omvat verschillende aspecten:

Juiste Timing: Data moet beschikbaar zijn precies wanneer het nodig is, niet te vroeg en niet te laat, om het proces niet te verstoren.

Realtime Toegang: Voor sommige processen is het essentieel om toegang te hebben tot realtime data, zodat beslissingen kunnen worden gebaseerd op de meest actuele informatie.

Synchroniciteit: In sommige gevallen moet data gesynchroniseerd zijn over verschillende systemen of afdelingen, zodat iedereen binnen het proces dezelfde informatie heeft.

Frequentie van Updates:
De data moet regelmatig en tijdig worden bijgewerkt om relevant en accuraat te blijven.

Tijdigheid is cruciaal omdat het directe invloed heeft op de efficiëntie, nauwkeurigheid en betrouwbaarheid van een proces. Onvoldoende tijdige data kan leiden tot vertragingen, fouten en suboptimale beslissingen, wat de algehele prestaties van het proces negatief kan beïnvloeden

Continuïteit

Continuïteit bij de beschikbaarheid van data binnen een proces verwijst naar het vermogen om de data ononderbroken beschikbaar te houden, zodat het proces soepel en zonder onderbrekingen kan verlopen. Dit betekent dat de data consistent en betrouwbaar beschikbaar is wanneer dat nodig is, zonder onderbrekingen of vertragingen. Continuïteit omvat verschillende aspecten:

Ononderbroken Toegang: Data moet altijd beschikbaar zijn zonder onverwachte uitval of onderbrekingen, zodat processen niet stilvallen.

Betrouwbaarheid: De systemen en infrastructuur die de data hosten moeten betrouwbaar zijn en een hoge uptime garanderen.

Redundantie: Er moeten back-ups en failover-mechanismen aanwezig zijn om te waarborgen dat data beschikbaar blijft, zelfs in het geval van storingen of systeemuitval.

Consistentie: De data moet consistent zijn over verschillende tijdstippen en toegangspunten, zodat er geen discrepanties zijn die het proces kunnen verstoren.

Disaster Recovery: Er moeten plannen en systemen aanwezig zijn om data snel te herstellen in geval van een ramp of grote storing, zodat de continuïteit van de processen niet in gevaar komt. Kortom, continuïteit bij de beschikbaarheid van data is cruciaal voor de stabiele en efficiënte werking van processen. Het zorgt ervoor dat processen niet worden onderbroken door technische problemen, en dat de benodigde data altijd beschikbaar is om de juiste beslissingen en acties te ondersteunen.

Robuustheid

Robuustheid bij de beschikbaarheid van data binnen een proces verwijst naar de mate waarin het systeem en de data bestand zijn tegen verstoringen, fouten en onverwachte omstandigheden, terwijl ze blijven functioneren zoals bedoeld. Het betekent dat de data en de systemen die deze beheren betrouwbaar en veerkrachtig zijn, zelfs onder stress of bij onverwachte gebeurtenissen. Robuustheid omvat verschillende aspecten:

Foutbestendigheid: Het systeem moet in staat zijn om te blijven functioneren ondanks het optreden van fouten, en moet fouten kunnen detecteren en corrigeren zonder dat dit leidt tot verlies van data of verstoring van het proces.

Weerstand tegen Verstoringen:
Het systeem moet bestand zijn tegen verschillende soorten verstoringen, zoals hardwarestoringen, softwareproblemen, en netwerkuitval, en moet mechanismen hebben om hiermee om te gaan.

Veerkracht: Het systeem moet snel kunnen herstellen van verstoringen of aanvallen en terugkeren naar de normale operationele staat zonder noemenswaardige downtime.

Redundantie: Er moeten redundante systemen en back-ups aanwezig zijn om te zorgen dat er altijd toegang is tot de data, zelfs als een deel van het systeem uitvalt.

Consistente Prestaties:
Het systeem moet consistente prestaties leveren, ook bij piekbelastingen of in minder ideale omstandigheden, zodat de data altijd beschikbaar blijft zoals verwacht.

Beveiliging: Het systeem moet beschermingen hebben tegen cyberaanvallen en onbevoegde toegang, om te voorkomen dat data beschadigd raakt of verloren gaat.

Kortom, robuustheid bij de beschikbaarheid van data zorgt ervoor dat processen kunnen blijven functioneren zonder onderbrekingen, zelfs onder moeilijke omstandigheden, en dat de integriteit en beschikbaarheid van data gewaarborgd blijft. Dit is essentieel voor de betrouwbaarheid en continuïteit van bedrijfsprocessen.

Toelichting integriteit (betrouwbaarheid)

Integriteit (betrouwbaarheid)
- ✓ *Juistheid*
- ✓ *Compleetheid*
- ✓ *Consistentie*
- ✓ *Validiteit (geldigheid)*
- ✓ *Continuiteit*
- ✓ *Actualiteit*
- ✓ *Precisie*
- ✓ *Plausibiliteit*
- ✓ *Traceerbaarheid*
- ✓ *Naleving*
- ✓ *Begrijpelijkheid*

Juistheid

Juistheid bij de integriteit van data binnen een proces verwijst naar de nauwkeurigheid en correctheid van de data, wat essentieel is voor het nemen van betrouwbare beslissingen en het uitvoeren van effectieve acties. Juistheid betekent dat de data precies en vrij van fouten is, en dat het een waarheidsgetrouwe weergave is van de werkelijkheid. Dit omvat verschillende aspecten:

Nauwkeurigheid: Data moet exact en precieze waarden bevatten die overeenkomen met de werkelijke omstandigheden of objecten die ze vertegenwoordigen.

Correctheid: Data moet vrij zijn van fouten, vergissingen en afwijkingen, zodat gebruikers kunnen vertrouwen op de informatie.

Validiteit: Data moet voldoen aan de gedefinieerde regels en standaarden voor het specifieke type data, bijvoorbeeld door juiste formaten en waardebereiken te hebben.

Volledigheid: Alle vereiste gegevens moeten aanwezig zijn zonder ontbrekende elementen, zodat er geen hiaten in de informatie zijn.

Consistentie: Data moet consistent zijn binnen verschillende systemen en over tijd, zonder conflicterende waarden die verwarring kunnen veroorzaken.

Juistheid is cruciaal voor de integriteit van data omdat onjuiste data kan leiden tot verkeerde beslissingen, inefficiënties, en potentieel schadelijke uitkomsten. In een proces waarin data centraal staat, zoals bij financiële transacties, medische diagnoses, of logistieke planning, kan de juistheid van de data directe invloed hebben op het succes en de betrouwbaarheid van het proces. Daarom zijn er vaak strikte controles en validatiemechanismen ingebouwd om de juistheid van de data te waarborgen.

Compleetheid

Compleetheid bij de integriteit van data binnen een proces verwijst naar de mate waarin alle vereiste gegevens aanwezig zijn zonder dat er informatie ontbreekt. Het betekent dat de dataset volledig is en dat alle noodzakelijke data-elementen beschikbaar zijn om het proces accuraat en effectief te ondersteunen. Compleetheid omvat verschillende aspecten:

Volledige Gegevenssets: Alle benodigde gegevensvelden en waarden moeten aanwezig zijn in de dataset. Er mogen geen essentiële data-elementen ontbreken die nodig zijn voor het uitvoeren van analyses, rapportages, of andere processtappen.

Verplichte Velden: Alle verplichte velden in de database of dataset moeten ingevuld zijn. Er mogen geen lege of null-waarden zijn waar data essentieel is voor de verwerking.

Integrale Gegevens: De gegevens moeten volledig zijn in de context van de gebruiksdoelen.

Bijvoorbeeld, een verhuizing moet niet alleen namen en adressen bevatten, maar ook contactinformatie voor nadere informatie

Tijdigheid van Compleetheid: De data moet op tijd en volledig zijn, zodat er geen vertragingen of onvolledigheden zijn op cruciale momenten binnen het proces.

Consistentie van Compleetheid:
Alle gerelateerde datasets moeten op elkaar afgestemd zijn qua volledigheid. Compleetheid is belangrijk voor de integriteit van data omdat incomplete data kan leiden tot misleidende analyses, onjuiste conclusies, en inefficiënties binnen het proces. Het kan ook problemen veroorzaken bij geautomatiseerde systemen die afhankelijk zijn van volledige datasets om correct te functioneren. Daarom is het vaak noodzakelijk om mechanismen te implementeren voor het controleren en valideren van de compleetheid van data, zoals invoercontroles, audits en kwaliteitscontroles.

Toelichting integriteit (betrouwbaarheid)

Integriteit (betrouwbaarheid)
- ✓ *Juistheid*
- ✓ *Compleetheid*
- ✓ *Consistentie*
- ✓ *Validiteit (geldigheid)*
- ✓ *Continuiteit*
- ✓ *Actualiteit*
- ✓ *Precisie*
- ✓ *Plausibiliteit*
- ✓ *Traceerbaarheid*
- ✓ *Naleving*
- ✓ *Begrijpelijkheid*

Consistentie

Consistentie bij de integriteit van data binnen een proces verwijst naar de eigenschap dat de data uniform en coherent is, zowel binnen een enkele dataset als tussen verschillende datasets en systemen. Dit betekent dat er geen tegenstrijdige of conflicterende informatie aanwezig is en dat dezelfde data-eenheden hetzelfde blijven over verschillende toepassingen en tijdstippen. Consistentie omvat verschillende aspecten:

Interne Consistentie: Binnen een enkele dataset moeten alle gegevens overeenkomen met de definities en regels die voor die dataset zijn vastgesteld. Bijvoorbeeld, als een klant in een database twee verschillende geboortedata heeft, is dat een inconsistentie.

Cross-Systeem Consistentie: Data die in verschillende systemen wordt gebruikt, moet overeenkomen. Bijvoorbeeld, een klantadres dat in zowel de Basis Registratie Personen als een vergunningensysteem wordt bijgehouden, moet in beide systemen hetzelfde zijn.

Tijdelijke Consistentie: Data moet over tijd consistent blijven, wat betekent dat wijzigingen correct en op alle relevante plaatsen worden doorgevoerd. Bijvoorbeeld, als een vergunningaanvrager verhuist, moet deze wijziging overal waar deze aanvrager wordt weergegeven, consistent worden bijgewerkt.

Referentiële Integriteit: Relaties tussen verschillende datasets moeten consistent zijn. Bijvoorbeeld, in een relationele database moeten de referenties tussen tabellen (zoals primaire en buitenlandse sleutels) intact en correct zijn.

Business Rules Consistentie: De data moet consistent zijn met de bedrijfsregels en logica. Bijvoorbeeld, de totale bestelwaarde in een orderverwerkingssyteem moet overeenkomen met de som van de individuele itemprijzen en eventuele belastingen of kortingen.

Consistentie is cruciaal voor de integriteit van data omdat inconsistente data kan leiden tot verwarring, verkeerde beslissingen en operationele problemen. Het kan ook het vertrouwen in de datasystemen en de beslissingen die daarop gebaseerd zijn, ondermijnen. Mechanismen om consistentie te waarborgen kunnen onder andere datavalidatieregels, synchronisatieprocessen, en controles zoals het gebruik van transacties in databases omvatten.

Validiteit (geldigheid)

Validiteit bij de integriteit van data binnen een proces verwijst naar de mate waarin de data correct en bruikbaar is binnen de context van het specifieke gebruiksdoel. Het betekent dat de data voldoet aan de gedefinieerde regels, normen en verwachtingen, en dat deze geschikt is voor de beslissingen en operaties waarvoor het wordt gebruikt. Validiteit omvat verschillende aspecten:

Correctheid van Waarden: Data moet waarden bevatten die logisch en binnen de verwachte bereik liggen. Bijvoorbeeld, een leeftijdsveld moet een positieve integer bevatten en binnen een plausibele grens (bijvoorbeeld 0-120 jaar) vallen.

Formaat en Structuur: Data moet het juiste formaat en de juiste structuur hebben. Bijvoorbeeld, een datavelden moeten voldoen aan het vereiste formaat (zoals YYYY-MM-DD voor datums) en geen ongeldige tekens bevatten.

Naleving van Bedrijfsregels: Data moet voldoen aan de bedrijfsregels en beleidsrichtlijnen. Bijvoorbeeld, een kortingspercentage moet binnen de toegestane grenzen vallen (bijvoorbeeld 0-100%).

Samenhang en Logische Verbanden: Data moet logisch samenhangend zijn binnen de context. Bijvoorbeeld, de datum van indiensttreding van een medewerker mag niet na de datum van ontslag liggen.

Type Consistentie: Data moet het juiste gegevenstype hebben. Bijvoorbeeld, numerieke waarden moeten in numerieke velden staan en tekstuele waarden in tekstvelden.

Validiteit is essentieel voor de integriteit van data omdat ongeldige data kan leiden tot onnauwkeurige analyses, verkeerde beslissingen en inefficiënties binnen het proces. Het waarborgen van validiteit kan worden bereikt door middel van diverse technieken, zoals:

Input Validatie: Controleren van data op het moment van invoer om ervoor te zorgen dat deze voldoet aan de gestelde eisen.

Data Audits: Periodieke controles en audits om de geldigheid van bestaande data te verifiëren.

Automatische Correcties: Gebruik van algoritmen en regels om ongeldige data automatisch te corrigeren of markeren voor handmatige beoordeling.

Educatie en Training: Zorgen dat medewerkers die data invoeren en beheren goed getraind zijn in het begrijpen en toepassen van de geldigheidsvereisten. Door de validiteit van data te waarborgen, kunnen organisaties erop vertrouwen dat hun data accuraat en bruikbaar is, wat cruciaal is voor de effectieve werking van hun processen.

Toelichting integriteit (betrouwbaarheid)

Integriteit (betrouwbaarheid)
- ✓ *Juistheid*
- ✓ *Compleetheid*
- ✓ *Consistentie*
- ✓ *Validiteit (geldigheid)*
- ✓ *Continuiteit*
- ✓ *Actualiteit*
- ✓ *Precisie*
- ✓ *Plausibiliteit*
- ✓ *Traceerbaarheid*
- ✓ *Naleving*
- ✓ *Begrijpelijkheid*

Continuïteit

Continuïteit bij de integriteit van data binnen een proces verwijst naar het vermogen om de integriteit van data ononderbroken te handhaven over tijd, zelfs in het geval van verstoringen, fouten of veranderingen. Dit betekent dat de data consistent, betrouwbaar en beschikbaar blijft, zodat processen soepel kunnen blijven verlopen zonder onderbrekingen of verlies van datakwaliteit. Continuïteit omvat verschillende aspecten:

Ononderbroken Beschikbaarheid:
Data moet altijd beschikbaar zijn wanneer het nodig is, zonder onverwachte onderbrekingen die de processen zouden kunnen verstoren.

Dataherstel: In geval van dataverlies of corruptie, moeten er effectieve herstelmechanismen zijn om de data snel en accuraat terug te brengen naar een consistente staat.

Back-up en Redundantie: Regelmatige back-ups en redundante systemen moeten aanwezig zijn om ervoor te zorgen dat er altijd een actuele kopie van de data beschikbaar is, zelfs als het primaire systeem faalt.

Consistente Data-updates: Alle wijzigingen en updates aan de data moeten consistent en volledig doorgevoerd worden over alle relevante systemen en processen, zodat er geen discrepanties ontstaan.

Beveiligingsmaatregelen: Robuuste beveiligingsmaatregelen moeten in plaats zijn om te voorkomen dat onbevoegde toegang of aanvallen de continuïteit en integriteit van de data in gevaar brengen.

Disaster Recovery Planning: Er moeten plannen en procedures zijn voor het omgaan met rampen of grote storingen, om te verzekeren dat de data-integriteit zo snel mogelijk wordt hersteld.

Continuïteit bij de integriteit van data is essentieel omdat onderbrekingen of inconsistenties in de data kunnen leiden tot fouten, inefficiënties en mogelijke schade aan het vertrouwen in de systemen en processen. Door de continuïteit van data-integriteit te waarborgen, kunnen organisaties ervoor zorgen dat hun processen altijd gebaseerd zijn op betrouwbare en accurate data, wat cruciaal is voor het nemen van geïnformeerde beslissingen en het handhaven van operationele efficiëntie.

Actualiteit

Actualiteit bij de integriteit van data binnen een proces verwijst naar de mate waarin de data up-to-date is, wat betekent dat de gegevens recent en relevant zijn voor het huidige moment en de actuele context. Actualiteit is essentieel voor het waarborgen dat beslissingen en acties gebaseerd zijn op de meest recente informatie. Dit omvat verschillende aspecten:

Tijdigheid van Updates: Data moet regelmatig en tijdig worden bijgewerkt om ervoor te zorgen dat het de huidige situatie weerspiegelt. Verouderde data kan leiden tot onjuiste conclusies en inefficiënte processen. Denk hierbij aan een bedrijf failliet is gegaan of verhuisd

Relevantie: Data moet niet alleen actueel zijn, maar ook relevant voor de huidige behoeften en doelen van het proces. Dit betekent dat alleen de meest recente en contextueel relevante informatie wordt gebruikt.

Frequentie van Veranderingen:
De snelheid waarmee data verandert moet overeenkomen met de frequentie van updates. Voor snel veranderende processen is frequentie actualisatie van data essentieel.

Synchronisatie: Data moet gesynchroniseerd zijn over verschillende systemen en databronnen, zodat alle gebruikers en processen werken met dezelfde actuele informatie.

Real-time Toegang: In sommige gevallen is real-time toegang tot data noodzakelijk, vooral in dynamische omgevingen waar omstandigheden snel kunnen veranderen, zoals in de WMO en Inkomen processen

Actualiteit is van cruciaal belang voor de integriteit van data omdat verouderde of irrelevante data kan leiden tot inefficiënties, fouten en slechte besluitvorming. Om actualiteit te waarborgen, kunnen organisaties verschillende strategieën implementeren:

Automatische Updates: Systemen die data automatisch bijwerken op basis van nieuwe input of gebeurtenissen. Binnen onze gemeente is dit bijvoorbeeld Datadistributie of Berichten verkeer

Monitoren en Alerts: Mechanismen om de actualiteit van data continu te monitoren en alerts in te stellen wanneer data verouderd raakt. Als voorbeeld is kan dit bijvoorbeeld adressen zijn welke in de Basisregistratie Adressen en Gebouwen waar splitsing of samenvoeging heeft plaatsgevonden

Data Governance: Beleidsmaatregelen en procedures die ervoor zorgen dat data regelmatig wordt herzien en bijgewerkt.

Gebruik van API's en Integraties:
Technologieën die zorgen voor real-time data-uitwisseling tussen systemen. Door de actualiteit van data te waarborgen, kunnen organisaties ervoor zorgen dat hun processen effectief blijven en gebaseerd zijn op de meest nauwkeurige en actuele informatie, wat essentieel is voor het nemen van geïnformeerde beslissingen en het handhaven van operationele efficiëntie. Een voorbeeld hiervan zijn de Common ground API's zoals de BRP Common Ground API die informatie van een burger direct uit de landelijke Basis Registrate Personen ophaalt

Toelichting integriteit (betrouwbaarheid)

Integriteit (betrouwbaarheid)
- ✓ *Juistheid*
- ✓ *Compleetheid*
- ✓ *Consistentie*
- ✓ *Validiteit (geldigheid)*
- ✓ *Continuiteit*
- ✓ *Actualiteit*
- ✓ *Precisie*
- ✓ *Plausibiliteit*
- ✓ *Traceerbaarheid*
- ✓ *Naleving*
- ✓ *Begrijpelijkheid*

Precisie

Precisie bij de integriteit van data binnen een proces verwijst naar de mate waarin de data nauwkeurig en exact is, zonder fouten, inconsistenties of ambiguïteiten. Het houdt in dat de data correct en gedetailleerd is, en dat het de gewenste mate van exactheid heeft voor het specifieke gebruik of de analyse ervan. Precisie omvat verschillende aspecten:

Nauwkeurigheid: Data moet correct en waarheidsgetrouw zijn, wat betekent dat het de werkelijke situatie accuraat weerspiegelt zonder overdrijving of onderbenutting.

Decimalen en Afrondingen: Bij numerieke data moet de precisie afgestemd zijn op de behoeften van het proces. Bijvoorbeeld, financiële data vereisen vaak een hoge precisie met betrekking tot decimalen.

Geen Dubbelzinnigheid: Data moet duidelijk en eenduidig zijn zonder dubbelzinnigheden of meervoudige interpretaties. Bijvoorbeeld, datums moeten worden weergegeven in een gestandaardiseerd formaat om verwarring te voorkomen.

Volledigheid van Informatie: Alle relevante details en contextuele informatie moeten aanwezig zijn om een volledig beeld te geven. Bijvoorbeeld, bij het registreren van een transactie moet alle nodige informatie, zoals datum, tijd, bedrag en betrokken partijen, worden vastgelegd.

Consistentie in Notatie: Data moet consistent zijn in termen van notatie en eenheid. Bijvoorbeeld, als eenheden gebruikt worden (zoals grammen, liters, euro's), moeten deze consistent worden toegepast over alle relevante data.

Precisie is van vitaal belang voor de integriteit van data omdat onnauwkeurige of onnauwkeurige data kan leiden tot verkeerde conclusies, fouten in analyses, en verlies van vertrouwen in de data en de processen die erop gebaseerd zijn. Om precisie te waarborgen, kunnen organisaties gebruik maken van verschillende methoden, waaronder:

Datavalidatie: Implementeren van regels en controles om de nauwkeurigheid van de ingevoerde data te controleren.

Data Cleansing: Het identificeren en corrigeren van fouten en inconsistenties in de data.

Gebruik van Referentiedata: Gebruik maken van betrouwbare en gevalideerde referentiedata om de nauwkeurigheid van de gegevens te verbeteren.

Training en Bewustwording: Het inwerken- en trainen van medewerkers en gebruikers over het belang van precisie en het juist vastleggen van data.

Door precisie te waarborgen, kunnen organisaties ervoor zorgen dat hun data betrouwbaar is en van hoge kwaliteit, wat essentieel is voor effectieve besluitvorming en het bereiken van de gewenste resultaten binnen hun processen.

Toelichting integriteit (betrouwbaarheid)

Integriteit (betrouwbaarheid)
- ✓ *Juistheid*
- ✓ *Compleetheid*
- ✓ *Consistentie*
- ✓ *Validiteit (geldigheid)*
- ✓ *Continuiteit*
- ✓ *Actualiteit*
- ✓ *Precisie*
- ✓ *Plausibiliteit*
- ✓ *Traceerbaarheid*
- ✓ *Naleving*
- ✓ *Begrijpelijkheid*

Plausibiliteit

Plausibiliteit bij de integriteit van data binnen een proces verwijst naar de mate waarin de data geloofwaardig en aannemelijk is, gezien de context en de verwachte patronen. Het betekent dat de data consistent is met wat redelijkerwijs verwacht kan worden en dat het logisch is binnen de bredere context van het proces of de situatie. Plausibiliteit omvat verschillende aspecten:

Logische Consistentie:
Data moet logisch consistent zijn en voldoen aan de gangbare verwachtingen en patronen binnen het betreffende domein. Bijvoorbeeld, een persoon van 150 jaar oud zou plausibel gezien onjuist zijn in de meeste contexten.

Overeenstemming met Historische Gegevens:
De data moet overeenstemmen met historische trends en gegevens. Bijvoorbeeld, als de omzet van een bedrijf plotseling drastisch stijgt zonder duidelijke verklaring, kan dit een plausibiliteitsprobleem zijn.

Geen Extreme Afwijkingen:
Data moet vrij zijn van extreme afwijkingen of anomalieën die niet kunnen worden verklaard door normale variaties of gebeurtenissen. Bijvoorbeeld, een plotselinge piek in temperatuurmetingen op een gematigde locatie in de winter kan onwaarschijnlijk zijn en vraagt om nader onderzoek.

Contextuele Relevantie:
Data moet relevant zijn binnen de bredere context van het proces of de situatie. Bijvoorbeeld, financiële gegevens moeten plausibel zijn binnen de context van de marktcondities en bedrijfsprestaties.

Consistentie met Externe Bronnen:
Indien mogelijk moet de data consistent zijn met informatie uit externe bronnen of referentiedata. Bijvoorbeeld, demografische gegevens moeten overeenstemmen met officiële statistieken.

Plausibiliteit is belangrijk voor de integriteit van data omdat het helpt om onjuiste of misleidende informatie te identificeren en te corrigeren voordat deze verder wordt gebruikt voor analyses of besluitvorming. Om plausibiliteit te waarborgen, kunnen organisaties verschillende methoden toepassen, zoals:

Data Validatie: Het implementeren van regels en controles om te controleren of de data plausibel is binnen de verwachte grenzen.

Gebruik van Referentiedata:
Het vergelijken van de data met betrouwbare externe bronnen of referentiedata om de plausibiliteit te beoordelen.

Analyse van Trends: Het analyseren van historische trends en gegevens om te controleren of de huidige data consistent is met verwachte patronen.

Menselijke Expertise: Het betrekken van experts binnen het betreffende domein binnen onze gemeente om de plausibiliteit van de data te beoordelen en te valideren.

Door plausibiliteit te waarborgen, kunnen wij binnen onze organisatie ervoor zorgen dat hun data geloofwaardig en betrouwbaar is, wat essentieel is voor het nemen van geïnformeerde beslissingen en het behouden van vertrouwen in de gegevens en processen.

Traceerbaarheid

Traceerbaarheid bij de integriteit van data binnen een proces verwijst naar het vermogen om de oorsprong en de volledige levenscyclus van de data te kunnen achterhalen. Het betekent dat elke wijziging, transformatie of beweging van de data gedocumenteerd en traceerbaar is, zodat het mogelijk is om de data terug te volgen naar de bron en te verifiëren of het proces van datavervorming betrouwbaar en legitiem is geweest. Traceerbaarheid omvat verschillende aspecten:

Bronverwijzing: Het bijhouden van informatie over de originele bron(nen) van de data, inclusief de datum en tijd van de invoer, de verantwoordelijke persoon of entiteit, en eventuele relevante metadata. Een voorbeeld hiervan zijn brondocumenten bij Basisregistraties

Wijzigingslogboeken: Het bijhouden van gedetailleerde wijzigingslogboeken die registreren wanneer en door wie elke wijziging aan de data is aangebracht, inclusief de aard van de wijziging en de reden ervoor.

Versiebeheer: Het bijhouden van verschillende versies van de data en het documenteren van de wijzigingen tussen elke versie, zodat gebruikers kunnen zien hoe de data in de loop van de tijd is geëvolueerd.

Audit Trails: Het vastleggen van audittrails die de volledige historie van data-activiteiten en -bewerkingen bijhouden, inclusief wie toegang heeft gehad tot de data en welke acties zijn ondernomen.

Keten van Vertrouwen:
Het vaststellen van een betrouwbare keten van vertrouwen die de volledige dataverwerkings- en overdrachtsstappen van begin tot eind documenteert.

Traceerbaarheid is van essentieel belang voor de integriteit van data omdat het transparantie, verantwoordingsplicht en vertrouwen in de data bevordert. Het stelt gebruikers in staat om de juistheid en betrouwbaarheid van de data te verifiëren, eventuele fouten op te sporen en te corrigeren, en mogelijke veiligheidsincidenten of misbruik te detecteren.

Het kan ook helpen bij het voldoen aan wettelijke en regelgevende vereisten met betrekking tot gegevensbeheer en -privacy. Om traceerbaarheid te waarborgen, moeten organisaties procedures en technologieën implementeren die de volledige dataverwerkings- en overdrachtsstappen vastleggen en documenteren. Dit omvat het gebruik van geautomatiseerde tools voor het bijhouden van wijzigingen, versiebeheer systemen, en sterke identiteits- en toegangsbeheerprocessen.

Toelichting integriteit (betrouwbaarheid)

Integriteit (betrouwbaarheid)
- ✓ *Juistheid*
- ✓ *Compleetheid*
- ✓ *Consistentie*
- ✓ *Validiteit (geldigheid)*
- ✓ *Continuiteit*
- ✓ *Actualiteit*
- ✓ *Precisie*
- ✓ *Plausibiliteit*
- ✓ *Traceerbaarheid*
- ✓ *Naleving*
- ✓ *Begrijpelijkheid*

Naleving

Naleving bij de integriteit van data binnen een proces verwijst naar het voldoen aan wettelijke, regelgevende en beleidsmatige vereisten met betrekking tot de verwerking, opslag, bescherming en gebruik van data. Het betekent dat organisaties en individuen zich houden aan de vastgestelde richtlijnen en normen om ervoor te zorgen dat data correct, eerlijk, veilig en vertrouwelijk wordt behandeld. Naleving omvat verschillende aspecten:

Wettelijke en Reglementaire Vereisten:
Het naleven van wetten, verordeningen en voorschriften die van toepassing zijn op specifieke soorten data, zoals de Algemene Verordening Gegevensbescherming (AVG), Wet BRP, Wet WMO etc. Het recht op inzage is in diverse wetten ook van toepassing

Industriestandaarden:
Het naleven van industriestandaarden en best practices voor gegevensbeheer en -beveiliging, zoals ISO 27001, gemeente specifiek ENSIA en BIO voor informatiebeveiliging.

Beleidsrichtlijnen en Interne Normen:
Het volgen van interne beleidsrichtlijnen en normen die zijn opgesteld de gemeente Oss zelf om de integriteit, vertrouwelijkheid en beschikbaarheid van data te waarborgen.

Privacybescherming:
Het waarborgen van de privacy van individuen door het naleven van privacyregels en het implementeren van passende beveiligingsmaatregelen voor het beschermen van persoonlijke gegevens.

Data Retentie en Vernietiging:
Het naleven van voorschriften met betrekking tot de bewaring en vernietiging van data, inclusief het vaststellen van bewaartermijnen en procedures voor het veilig verwijderen van data wanneer deze niet langer nodig is. (het recht om vergeten te worden)

Naleving is van cruciaal belang voor de integriteit van data omdat het de rechten en belangen van individuen beschermt, de risico's van gegevensinbreuken vermindert en het vertrouwen van stakeholders in de organisatie versterkt. Het niet naleven van nalevingsvereisten kan leiden tot juridische sancties, boetes, reputatieschade en verlies van vertrouwen van klanten en partners. Om naleving te waarborgen, moeten wij in onze organisatie procedures, beleidslijnen en controles implementeren die voldoen aan relevante wetten en normen.

Dit omvat het regelmatig evalueren van nalevingsvereisten, het inwerken en regelmatig trainen van onze medewerkers over hun verantwoordelijkheden met betrekking tot naleving, en het regelmatig uitvoeren van audits en controles om te controleren of aan de vereisten wordt voldaan.

Begrijpelijkheid

Begrijpelijkheid bij de integriteit van data binnen een proces verwijst naar de mate waarin de data gemakkelijk te begrijpen en te interpreteren is door de gebruikers die deze data nodig hebben. Het betekent dat de data duidelijk en helder gepresenteerd wordt, zodat gebruikers de betekenis, context en implicaties ervan kunnen begrijpen zonder verwarring of misinterpretatie. Begrijpelijkheid omvat verschillende aspecten:

Duidelijke Presentatie:
Data moet op een gestructureerde en overzichtelijke manier worden gepresenteerd, zodat gebruikers snel de relevante informatie kunnen vinden en begrijpen.

Gebruik van Begrijpelijke Taal:
Het gebruik van eenvoudige en begrijpelijke taal, vrij van technisch jargon of complexe terminologie, om de communicatie te vergemakkelijken.

Contextuele Informatie:
Het verstrekken van relevante contextuele informatie die gebruikers helpt om de data te begrijpen en de betekenis ervan te interpreteren binnen de bredere context van het proces of de situatie.

Visualisatie:
Het gebruik van grafieken, diagrammen, en andere visuele hulpmiddelen om data op een intuïtieve manier weer te geven, waardoor gebruikers snel patronen, trends en relaties kunnen identificeren.

Documentatie en Uitleg:
Het verstrekken van gedetailleerde documentatie en uitleg over de betekenis en de herkomst van de data, evenals eventuele definities of berekeningsmethoden die van toepassing zijn.

Begrijpelijkheid is belangrijk voor de integriteit van data omdat het ervoor zorgt dat gebruikers de data correct kunnen interpreteren en effectief kunnen gebruiken voor besluitvorming en actie. Als data niet begrijpelijk is, kan dit leiden tot misinterpretaties, foutieve conclusies, en inefficiënties in het proces. Daarnaast kan gebrek aan begrijpelijkheid het vertrouwen van gebruikers in de data verminderen en de acceptatie van nieuwe systemen of processen belemmeren.

Om begrijpelijkheid te waarborgen, moeten we binnen de gemeente Oss aandacht besteden aan de presentatie en communicatie van data en ervoor zorgen dat gebruikers voldoende ondersteuning en uitleg krijgen om de data correct te kunnen interpreteren.

Dit kan onder meer inhouden: het bieden van training en educatie aan gebruikers (datageletterdheid), het implementeren van gebruiksvriendelijke interfaces, en het verstrekken van duidelijke documentatie en richtlijnen voor het gebruik van de data.

Toelichting vertrouwelijkheid

Vertrouwelijkheid
✓ *Exclusiviteit*
✓ *Privacy*

Exclusiviteit (vetrouwelijkheid)

Exclusiviteit bij de vertrouwelijkheid van data binnen een proces verwijst naar de mate waarin de toegang tot de data beperkt is tot geautoriseerde gebruikers of entiteiten, en dat de data niet beschikbaar is voor onbevoegde partijen. Het houdt in dat de data alleen wordt gedeeld met degenen die een legitieme behoefte hebben om toegang te hebben tot de informatie en dat er mechanismen zijn ingesteld om ongeautoriseerde toegang te voorkomen. Exclusiviteit omvat verschillende aspecten:

Toegangscontrole: Het implementeren van strikte toegangscontrolemechanismen om ervoor te zorgen dat alleen geautoriseerde gebruikers toegang hebben tot de data, en dat elke toegang wordt geregistreerd en gecontroleerd.

Gebruikersrechten: Het toewijzen van specifieke rechten en privileges aan gebruikers op basis van hun rol en verantwoordelijkheden, zodat ze alleen toegang hebben tot de data die relevant is voor hun taken.

Versleuteling: Het versleutelen (bijvoorbeeld Zivver)van gevoelige data tijdens opslag en overdracht om ervoor te zorgen dat zelfs als de data wordt onderschept, het niet leesbaar is voor ongeautoriseerde partijen.

Fysieke Beveiliging: Het implementeren van fysieke beveiligingsmaatregelen, zoals het beperken van de toegang tot serverruimtes of het gebruik van bijv. biometrische identificatie, om te voorkomen dat onbevoegden fysieke toegang krijgen tot de data.

Geheimhoudingsverklaringen en Overeenkomsten:
Het afdwingen van geheimhoudingsverklaringen en (lever- en verwerkers) overeenkomsten met medewerkers, partners en andere entiteiten die toegang hebben tot de data, om ervoor te zorgen dat ze de vertrouwelijkheid van de informatie respecteren.

Exclusiviteit is essentieel voor de vertrouwelijkheid van data omdat het ervoor zorgt dat gevoelige informatie beschermd blijft tegen ongeoorloofde openbaarmaking, diefstal of misbruik. Het kan helpen om privacy te waarborgen, intellectueel eigendom te beschermen en de naleving van wet- en regelgeving met betrekking tot gegevensbescherming te handhaven. Om exclusiviteit te waarborgen, moeten organisaties zorgvuldig bepalen wie toegang heeft tot welke data, en ervoor zorgen dat er passende controles en beveiligingsmaatregelen worden geïmplementeerd om de vertrouwelijkheid van de informatie te beschermen. Dit omvat het regelmatig evalueren en bijwerken van toegangsrechten, het monitoren van gebruikersactiviteiten, en het regelmatig uitvoeren van beveiligingsaudits en controles.

Privacy

Privacy bij de vertrouwelijkheid van data binnen een proces verwijst naar het recht en de verwachting van individuen dat hun persoonlijke informatie wordt beschermd tegen ongeoorloofde toegang, gebruik, openbaarmaking of misbruik. Het houdt dat wij in de gemeente Oss verantwoordelijk zijn voor het waarborgen van de vertrouwelijkheid en integriteit van persoonlijke gegevens, en dat ze de privacyrechten van individuen respecteren en naleven. Privacy omvat verschillende aspecten:

Verzameling en Gebruik van Gegevens:
Het beperken van de verzameling en het gebruik van persoonlijke gegevens tot legitieme doeleinden en alleen met de toestemming van de betrokken personen.

Beveiliging van Gegevens:
Het implementeren van passende beveiligingsmaatregelen om persoonlijke gegevens te beschermen tegen ongeautoriseerde toegang, misbruik, verlies of diefstal.

Transparantie en Informatieverstrekking:
Het verstrekken van duidelijke en begrijpelijke informatie aan individuen over hoe hun persoonlijke gegevens worden verzameld, gebruikt, opgeslagen en gedeeld.

Toestemmingsbeheer:
Het verkrijgen van de expliciete toestemming van individuen voordat hun persoonlijke gegevens worden verwerkt, en het respecteren van hun recht om deze toestemming op elk moment in te trekken.

Rechten van Individuen:
Het erkennen en respecteren van de privacyrechten van individuen, zoals het recht op toegang tot hun persoonlijke gegevens, het recht op rectificatie van onjuiste informatie, en het recht op verwijdering van gegevens (het recht om vergeten te worden).

Privacy is van cruciaal belang voor de vertrouwelijkheid van data omdat het individuen beschermt tegen inbreuken op hun persoonlijke levenssfeer en de mogelijkheid biedt om controle te hebben over hun persoonlijke informatie. Het helpt ook om vertrouwen op te bouwen tussen de gemeente en haar klanten, en om te voldoen aan wet- en regelgeving met betrekking tot gegevensbescherming, zoals de Algemene Verordening Gegevensbescherming (AVG) in Europa. Om privacy te waarborgen, moeten wij bij de gemeente Oss zorgvuldig omgaan met persoonlijke gegevens, de nodige maatregelen nemen om de vertrouwelijkheid en beveiliging ervan te waarborgen, en transparant communiceren over hun privacybeleid en -praktijken.
Dit omvat het implementeren van privacybeleid en -procedures, het trainen- en inwerken van medewerkers over privacykwesties, het uitvoeren van privacy-impactbeoordelingen, en het regelmatig evalueren en bijwerken van privacypraktijken in overeenstemming met veranderende wet- en regelgeving en beste praktijken.