

HANDREIKING DATACLASSIFICATIE

**Een van de producten van de operationele variant van de Baseline
Informatiebeveiliging Nederlandse Gemeenten (BIG)**



Colofon

Naam document

Handreiking Dataclassificatie

Versienummer

1.0

Versiedatum

oktober 2013

Versiebeheer

Het beheer van dit document berust bij de Informatiebeveiligingsdienst voor gemeenten (IBD).

Copyright

© 2013 Kwaliteitsinstituut Nederlandse Gemeenten (KING).

Alle rechten voorbehouden. Verveelvoudiging, verspreiding en gebruik van deze uitgave voor het doel zoals vermeld in deze uitgave is met bronvermelding toegestaan voor alle gemeenten en overheidsorganisaties.

Voor commerciële organisaties wordt hierbij toestemming verleend om dit document te bekijken, af te drukken, te verspreiden en te gebruiken onder de hiernavolgende voorwaarden:

1. KING wordt als bron vermeld;
2. het document en de inhoud mogen commercieel niet geëxploiteerd worden;
3. publicaties of informatie waarvan de intellectuele eigendomsrechten niet bij de verstrekker berusten, blijven onderworpen aan de beperkingen opgelegd door de KING;
4. ieder kopie van dit document, of een gedeelte daarvan, dient te zijn voorzien van de in deze paragraaf vermelde mededeling.

Rechten en vrijwaring

KING is zich bewust van haar verantwoordelijkheid een zo betrouwbaar mogelijke uitgave te verzorgen. Niettemin kan KING geen aansprakelijkheid aanvaarden voor eventueel in deze uitgave voorkomende onjuistheden, onvolledigheden of nalatigheden. KING aanvaardt ook geen aansprakelijkheid voor enig gebruik van voorliggende uitgave of schade ontstaan door de inhoud van de uitgave of door de toepassing ervan.

In samenwerking met

De producten van de operationele variant van de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG) worden vervaardigd in samenwerking met:



Voorwoord

De IBD is een gezamenlijk initiatief van de Vereniging van Nederlandse Gemeenten (VNG) en het Kwaliteitsinstituut Nederlandse Gemeenten (KING) en actief sinds 1 januari 2013. Aanleiding voor de oprichting van de IBD vormen enerzijds de leerpunten uit een aantal grote incidenten op informatiebeveiligingsvlak en anderzijds de visie Digitale Overheid 2017.

De IBD is er voor alle gemeenten en richt zich op bewustwording en concrete ondersteuning om gemeenten te helpen hun informatiebeveiliging naar een hoger plan te tillen.

De IBD heeft drie doelen:

1. het preventief en structureel ondersteunen van gemeenten bij het opbouwen en onderhouden van bewustzijn als het gaat om informatiebeveiliging.
2. het leveren van integrale coördinatie en concrete ondersteuning op gemeente specifieke aspecten in geval van incidenten en crisissituaties op het vlak van informatiebeveiliging.
3. het bieden van gerichte projectmatige ondersteuning op deelgebieden om informatiebeveiliging in de praktijk van alle dag naar een hoger plan te tillen. De ondersteuning die de IBD biedt bij het ICT-beveiligingsassessment DigiD is een voorbeeld van zo'n project.

Hoe realiseert de IBD haar doelen?

Om invulling te kunnen geven aan haar doelen is door de IBD op basis van de Baseline Informatiebeveiliging Rijksdienst (BIR) een vertaalslag gemaakt naar een baseline voor de gemeentelijke markt. Deze Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG) betreft twee varianten, een Strategische- én een Tactische Baseline. Beide varianten van de BIG zijn beschikbaar voor alle gemeenten op de community van de IBD, zodat door iedere gemeente tot implementatie van de BIG kan worden overgegaan. Bestuur en management hebben met deze baseline een instrument in handen waarmee zij in staat zijn om te meten of de organisatie 'in control' is op het gebied van informatiebeveiliging. Om de implementatie van de Strategische en Tactische Baseline te ondersteunen, zijn door de IBD in samenwerking met de Taskforce Bestuur en Informatieveiligheid Dienstverlening producten ontwikkeld op operationeel niveau. Dit heeft een productenportfolio opgeleverd, genaamd de Operationele Baseline Nederlandse Gemeenten. Onderhavig product is onderdeel van het productenportfolio.

Naast een productenportfolio, heeft de IBD voor gemeenten ook een dienstenportfolio ontwikkeld. Voor een volledig overzicht van het producten- en dienstenportfolio, kunt u terecht op de website van de IBD.

De gemeente is zelf verantwoordelijk voor het opstellen en/of uitvoeren en/of handhaven van de regels. Hierbij geldt:

- Er is wetgeving waar altijd aan voldaan moet worden, zoals niet uitputtend: GBA, SUWI, BAG en PUN, maar ook de archiefwet.
- Er is een gemeenschappelijk normenkader als basis: de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG).
- De gemeente stelt dit normenkader vast, waarbij er ruimte is voor afweging en prioritering op basis van het 'pas toe of leg uit' principe.

Leeswijzer

Dit product maakt onderdeel uit van de operationele variant van de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG).

Doel

Dit document bevat een good practice voor (data)classificatie. Data betekent in dit verband alle gegevens en informatie, ongeacht het medium waarop deze opgeslagen wordt en ongeacht de presentatie daarvan.

Doelgroep

Dit document is van belang voor systeemeigenaren en informatiemanagers.

Relatie met overige producten

- Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG)
 - Strategische variant van de Baseline Informatiebeveiliging Nederlandse Gemeenten
 - Tactische variant van de Baseline Informatiebeveiliging Nederlandse Gemeenten
- Voorbeeld Informatiebeveiligingsbeleid Gemeenten
- GAP-analyse

Maatregelen tactische variant Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG)

7.2

Inhoud

1	Inleiding	6
2	Classificatie van data	7
2.1	Risicoanalyse en restrisico's	7
3	Beleidskaders voor classificatie	9
4	Principes voor classificatie	11
5	Beveiligingseisen per classificatieniveau	12
5.1	Beschikbaarheid	12
5.2	Integriteit	13
5.3	Vertrouwelijkheid	15
	Stap 1: Wettelijke eisen	17
	Stap 2: Verantwoordelijkheden t.a.v. data	17
	Stap 3: Analyse kritische bedrijfsprocessen	18
	Stap 4: Afweging: criteria bij het bepalen van het classificatieniveau	19
	Stap 5: Het resultaat	20
	Bijlage 1: Classificatie leidraad	21
	Bijlage 2: Classificatie vragenlijsten	22
	B – Vragenlijst beschikbaarheid	23
	I – Vragenlijst integriteit	25
	V – Vragenlijst vertrouwelijkheid	27
	Bijlage 3: Waarderingschaal	29

1 Inleiding

Dit document bevat een good practice voor (data)classificatie. In dit document wordt alleen gepraat over classificatie, maar rubricering wordt binnen het vakgebied ook vaak gebruikt. Data betekent in dit verband alle gegevens en informatie, ongeacht het medium waarop deze opgeslagen wordt en ongeacht de presentatie daarvan. Classificatie gaat in dit geval niet dieper dan een proces of een systeem. De in deze handreiking genoemde niveaus en (bewaar)termijnen zijn een voorstel en komen uit verschillende brondocumenten, waaronder: wetgeving, PVIB patronen, een gemeente en de strategische variant van de Baseline Informatiebeveiliging Nederlandse Gemeenten.

Classificatie van data geeft antwoord over de hoeveelheid maatregelen die genomen moeten worden om die data adequaat te beschermen en geeft ook antwoord op de vraag of de data binnen of buiten de baseline valt.

De maatregel dataclassificatie of rubricering komt voort uit de tactische variant van de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG), hoofdstuk 7.2.

Doelstelling handreiking

De hier voorgestelde classificatie handleiding beschrijft een good practice voor classificatie van informatie. De leidraad biedt handvatten om een classificatiesysteem te ontwikkelen of te verbeteren en deze te implementeren.

Belang van classificatie

De mogelijke schade die een dreiging (bijv. misbruik door oneigenlijke toegang) kan toebrengen aan bepaalde informatie en de kans dat het optreedt, kan met een risicoanalyse worden geëvalueerd. Het management dient vervolgens aan te geven welke risico's aanvaardbaar zijn en welke met maatregelen moeten worden afgedekt. Het gebruik van standaard risicoanalyse hulpmiddelen is vaak een tijdrovend en abstract traject. De voorgestelde classificatiemethodiek geeft een snelle indicatie van het belang van de informatie(systemen) en is daarmee een basis voor een risicoanalyse. Na de classificatie kunnen de juiste maatregelen getroffen worden waardoor enerzijds inbreuken op de veiligheid worden voorkomen en anderzijds daarvoor niet nodeloos veel inspanning getroost wordt.

2 Classificatie van data

Informatiebeveiliging is het geheel van maatregelen en procedures om informatie te beschermen. Het doel is: waarborgen van de continuïteit, integriteit en vertrouwelijkheid van informatie en de informatievoorziening en het beperken van de gevolgen van eventuele beveiligingsincidenten.

Het beschermingsniveau van data wordt uitgedrukt in classificatieniveaus voor beschikbaarheid, integriteit en vertrouwelijkheid van informatie:

- **Beschikbaarheid:** hoeveel en wanneer data toegankelijk is en gebruikt kan worden. De onderscheiden niveaus zijn: niet nodig; noodzakelijk; belangrijk en essentieel.
- **Integriteit:** het in overeenstemming zijn van informatie met de werkelijkheid en dat niets ten onrechte is achtergehouden of verdwenen (juistheid, volledigheid en tijdigheid). De onderscheiden niveaus zijn: niet zeker; beschermd; hoog en absoluut.
- **Vertrouwelijkheid:** de bevoegdheden en de mogelijkheden tot muteren, kopiëren, toevoegen, vernietigen of kennisnemen van informatie voor een gedefinieerde groep van gerechtigden. De onderscheiden niveaus zijn: openbaar; bedrijfsvertrouwelijk, vertrouwelijk en geheim.

Het toekennen van classificatieniveaus aan data en/of informatiesystemen is van groot belang, omdat daarmee het (vereiste) beschermingsniveau kenbaar gemaakt wordt. Aan de hand hiervan kan worden bepaald welke beveiligingseisen gelden en welke maatregelen moeten worden genomen. Dit is bijvoorbeeld relevant voor beheerders die lang niet altijd bekend zijn met de inhoud en dus de waarde van data, maar wel worden geacht adequate beschermingsmaatregelen te treffen. De volgende factoren oefenen invloed uit op de adequate beveiligingsmaatregelen: beleidsuitgangspunten, architectuurprincipes, beveiligingseisen (en hoe deze te interpreteren).

Met de invoering van de Baseline Informatiebeveiliging voor Gemeenten is het basis beveiligingsniveau bepaald dat geldt voor de gehele bedrijfsvoering van een gemeente. Hierdoor moeten alleen processen en systemen onderzocht worden waarvan verwacht wordt dat deze meer beveiligingsmaatregelen nodig hebben dan de Baseline.

Met een classificatiemethode kan bepaald worden of het proces of systeem binnen of buiten baseline valt. Indien de classificatie hoger dan vertrouwelijk is, dan zijn extra maatregelen nodig. Soms zijn deze maatregelen al genomen als application control (binnen de applicatie). Soms zijn deze extra maatregelen al uitgewerkt door een uitgevoerde risicoanalyse van een andere gemeente of er wordt binnen de gemeente een risicoafweging gemaakt door het uitvoeren van een risicoanalyse met als resultaat meer passende maatregelen.

2.1 Risicoanalyse en restrisico's

Een gemeente die informatie verwerkt en daarbij informatiesystemen gebruikt loopt bepaalde risico's doordat die informatie en systemen kwetsbaar zijn voor dreigingen van binnen en van buiten.

Het uitvoeren van een risicoanalyse ondersteunt het management bij het vaststellen van de risico's die worden gelopen en hoe groot die risico's zijn. Daarmee kan vervolgens bepaald worden welke beveiligingsmaatregelen getroffen moeten worden om de risico's terug te dringen. Vooral bij de vertaling van risico naar maatregel is classificatie een belangrijk hulpmiddel om de ernst van een risico en de reikwijdte van een maatregel te kunnen bepalen. De voorgestelde Classificatie handreiking kan beschouwd worden als een vereenvoudigde vorm van een risicoanalyse.

Bij een risicoanalyse worden bedreigingen benoemd en in kaart gebracht. Per bedreiging wordt de kans van het optreden ervan bepaald en wordt vervolgens berekend wat de schade is die op zou kunnen optreden als een bedreiging zich daadwerkelijk voordoet.

De bedoeling van een risicoanalyse is dat er na de analyse wordt vastgesteld op welke wijze de risico's beheerst kunnen worden, of teruggebracht tot een aanvaardbaar niveau: het treffen van informatiebeveiligingsmaatregelen. Daarbij wordt naast een risicoanalyse ook een kosten en baten analyse uitgevoerd. Op voorhand hoeft niet ieder risico te worden afgedekt: wanneer de kosten van de maatregelen om een risico te beperken hoger zijn dan de mogelijke schade, dan kan besloten worden het risico te accepteren.

Het is de eigenaar/houder van de gegevens die bepaalt of deze classificatie juist is, maar ook of dat beargumenteerd van de aan deze classificatie gekoppelde maatregelen kan worden afgeweken, omdat het restrisico acceptabel is.

3 Beleidskaders voor classificatie

In dit hoofdstuk worden aanvullende beleidskaders als voorbeeld weergegeven welke als apart beleid naast het informatiebeveiligingsbeleid van de gemeente uitgegeven kunnen worden.

Voorbeeld beleid:

Het informatiebeveiligingsbeleid van de gemeente <gemeentenaam> beschrijft globaal de normen voor beschikbaarheid, integriteit en vertrouwelijkheid van informatie.

De onderscheiden niveaus van beschikbaarheid zijn:

- Niet nodig: De gegevens kunnen zonder gevolgen langere tijd niet beschikbaar zijn. Schending van beschikbaarheid heeft geen gevolgschade.
- Noodzakelijk: De informatie of service mag incidenteel uitvallen, het bedrijfsproces staat incidentele uitval toe. De continuïteit zal op redelijke termijn moeten worden hervat. Schending van deze classificatie kan enige¹ (in)directe schade toebrengen.
- Belangrijk: De informatie of service mag bijna nooit uitvallen, het bedrijfsproces staat nauwelijks uitval toe. De continuïteit zal snel moeten worden hervat. Schending van deze classificatie kan serieuze² (in)directe schade toebrengen.
- Essentieel: De informatie of service mag alleen in zeer uitzonderlijke situaties uitvallen, bijvoorbeeld als gevolg van een calamiteit, het bedrijfskritische bedrijfsproces staat eigenlijk geen uitval toe. De continuïteit zal zeer snel moeten worden hervat. Schending van integriteit kan (zeer) grote³ schade toebrengen.

De onderscheiden niveaus van integriteit zijn:

- Niet zeker: Deze informatie mag worden veranderd. Geen extra bescherming van integriteit noodzakelijk. Schending van integriteit heeft geen gevolgschade.
- Beschermd: Het bedrijfsproces dat gebruik maakt van deze informatie staat enkele (integriteits-)fouten toe. Een basisniveau van beveiliging is noodzakelijk. Schending van deze classificatie kan enige (in-)directe schade toebrengen.
- Hoog: Het bedrijfsproces dat gebruik maakt van deze informatie staat zeer weinig (integriteits-)fouten toe. Bescherming van integriteit is absoluut noodzakelijk. Schending van deze classificatie kan serieuze (in)directe schade toebrengen.
- Absoluut: Het bedrijfsproces dat gebruik maakt van deze informatie staat geen (integriteits-)fouten toe. Schending van integriteit kan (zeer) grote schade toebrengen.

De onderscheiden niveaus van vertrouwelijkheid zijn:

- Openbaar: Alle informatie die algemeen toegankelijk is voor een ieder. Er is geen schending van deze classificatie mogelijk.
- Bedrijfsvertrouwelijk: Informatie die toegankelijk mag of moet zijn voor alle medewerkers van de eigen organisatie(s). Vertrouwelijkheid is gering. Schending van deze classificatie kan enige (in)directe schade toebrengen.
- Vertrouwelijk: Informatie die alleen toegankelijk mag zijn voor een beperkte groep gebruikers⁴. De informatie wordt ter beschikking gesteld op basis van vertrouwen. Schending van deze classificatie kan serieuze (in)directe schade toebrengen.

¹²³ Voor uitleg over 'enige', 'serieuze' en 'zeer grote' zie bijlage 3

⁴ Onder de term 'beperkte groep gebruikers' in de definitie van 'vertrouwelijk' wordt een verzameling identiteiten met een specifieke en gemeenschappelijke taak en/of functie bedoeld; niet het lid zijn van een bepaalde dienst of deelgemeente.

INFORMATIE BEVEILIGINGS DIENST

- Geheim: Dit betreft gevoelige informatie die alleen toegankelijk mag zijn voor de direct geadresseerde. Schending van deze classificatie kan zeer grote schade toebrengen.

4 Principes voor classificatie

De volgende principes zijn het uitgangspunt voor (data) classificatie:

- De classificatietabel heeft betrekking op alle in beheer zijnde gegevensverzamelingen, gegevensdragers, informatiesystemen, servers en netwerkcomponenten.
- Informatie kan meer of minder gevoelig of kritisch zijn. Voor bepaalde informatie kan een extra niveau van bescherming of een speciale verwerking nodig zijn. Als een informatiesysteem daarvoor maatregelen (applicatie controls) genomen heeft om delen van de systeeminformatie die hoger geclassificeerd is adequaat te beschermen op record of schermniveau, dan kan een systeem als geheel lager ingeschaald worden binnen de tabel en daarmee bijvoorbeeld alsnog binnen de baseline vallen.
- De eigenaar van de gegevens (veelal ook de proceseigenaar) bepaalt het vereiste beschermingsniveau (classificatie). Indien sprake is van wettelijke eisen wordt dit expliciet aangegeven. De eigenaar van de gegevens bepaalt tevens wie toegang krijgt tot welke gegevens.
- Er wordt gestreefd naar een zo 'laag' mogelijk classificatieniveau; te hoge classificatie leidt tot onnodige kosten. Bovendien dient informatie in beginsel voor zoveel mogelijk mensen beschikbaar zijn in het kader van een transparante overheid.
- Het object van classificatie is informatie. De classificatie die door de soort informatie bepaald wordt geldt ook voor het hogere niveau van informatiesystemen (of informatieservices), dat wil zeggen dat als een systeem geheime informatie verwerkt het hele systeem als geheim wordt aangemerkt tenzij voor dat hogere niveau maatregelen genomen zijn binnen het informatiesysteem. Alle classificaties van alle bedrijfskritische systemen zijn centraal vastgelegd door de eigenaren en dienen jaarlijks gecontroleerd te worden door de CISO.

In alle gevallen kan de eigenaar van de gegevens zich voor het classificeren laten ondersteunen door beveiligingsspecialisten, zoals de CISO.

Het uitgangspunt is de BIG. Echter als er meer maatregelen nodig zijn dan dienen de te nemen maatregelen te worden afgestemd op de risico's, waarbij rekening dient te worden gehouden met technische mogelijkheden en de kosten van de te nemen maatregelen. Dit is vaak situatie-afhankelijk. Naarmate de gegevens een gevoeliger karakter hebben, of gezien de context waarin ze gebruikt worden een groter risico inhouden, dienen zwaardere eisen aan de beveiliging van die gegevens te worden gesteld. In het algemeen kan worden gesteld dat indien met naar verhouding geringe extra kosten meer beveiliging kan worden bewerkstelligd dit als 'passend' kan worden beschouwd. Extra beveiliging is echter niet meer passend, indien de kosten voor het mitigeren van de risico's disproportioneel hoog zijn. Kort gezegd: risico's en de te nemen maatregelen dienen in balans te zijn.

5 Beveiligingseisen per classificatieniveau

5.1 Beschikbaarheid

Beschikbaarheid stelt in tegenstelling tot integriteit en vertrouwelijkheid geen eisen aan de inhoud van de data. Er gelden daarom geen bijzondere maatregelen voor authenticatie, autorisatie, monitoring en beveiliging, zoals voor integriteit en vertrouwelijkheid (zie volgende paragrafen). Aangezien de normen voor beschikbaarheid verschillen per service moet het classificatieniveau voor beschikbaarheid altijd worden gespecificeerd.

Definitie

Beschikbaarheid is gedefinieerd als 'eigenschappen van het geheel van ICT-diensten, systemen, componenten en gegevensdragers die van invloed zijn op de tijd dat het product of de dienst (en daarmee informatie) beschikbaar is voor de geautoriseerde gebruiker, op de momenten dat het beschikbaar moet zijn'. Beschikbaarheid wordt gemeten aan de hand van de Mean Time Between Failures (MTBF). Dit is de gemiddelde tijd tussen het herstel van het ene incident en het optreden van het volgende incident.

De in de onderstaande tabel genoemde waarden zijn een voorbeeld, deze waarden moeten door de gemeente zelf bepaald worden.

Beveiligingsnormen:

De normen voor de kantoor Automatisering (KA), Intranet van de gemeente <gemeentenaam> en de toegevoegde diensten zijn *(let op, dit kan per systeem / klasse worden ingevuld)*:

KA (basis en plus applicaties): 99,5% beschikbaarheid op werkdagen tussen 7:30 en 18:00 Intranet <gemeentenaam>: 99,5% beschikbaarheid op werkdagen tussen 7:30 en 18:00

Klasse Noodzakelijk		
Werktijden	Van 08:00 tot 17:00 uur op maandag t/m vrijdag behoudens algemeen erkende feestdagen.	
Beschikbaarheid tijdens werktijd	99,6%	(min.)
Beschikbaarheid buiten werktijd	96,1%	(min.)
MTBF	100 dagen	(min.)
MTTR (voor storingen langer dan 3	4 uur	(max.)
Aantal storingen:		
3 Minuten of korter	4 per maand	(max.)
Langer dan 3 minuten	1 per maand	(max.)

Klasse Belangrijk		
Werktijden	Van 07:00 tot 21:00 uur op maandag t/m vrijdag behoudens algemeen erkende feestdagen.	
Beschikbaarheid tijdens werktijd	99,6%	(min.)
Beschikbaarheid buiten werktijd	96,1%	(min.)

INFORMATIE BEVEILIGINGS DIENST

MTBF	100 dagen	(min.)
MTTR (voor storingen langer dan 3	4 uur	(max.)
Aantal storingen:		
3 Minuten of korter	2 per maand	(max.)
Langer dan 3 minuten	1 per 2 maanden	(max.)

Klasse Essentieel		
Werktijden	24 uur per dag, 7 dagen per week, behoudens gepland onderhoud.	
Beschikbaarheid	99,9%	(min.)
MTBF	200 dagen	(min.)
MTTR (voor storingen langer dan 3	4 uur	(max.)
Aantal storingen:		
3 Minuten of korter	1 per maand	(max.)
Langer dan 3 minuten	1 per halfjaar	(max.)

5.2 Integriteit

Het onderwerp integriteit valt normaliter in twee delen uiteen: de integriteit van data communicatie en opslag enerzijds (d.w.z. niet gerelateerd aan het gemeentelijke proces zelf), en de integriteit van de informatie in de applicaties of fysiek (d.w.z. gerelateerd aan het gemeentelijke proces zelf). Integriteit gekoppeld aan de applicatie is altijd situatie afhankelijk en afhankelijk van de eisen van een specifiek proces. Voor de functionele integriteit van de informatievoorziening wordt een minimale set van normen opgesteld waarbij er per dienst en/of applicatie nadere afspraken gemaakt kunnen worden.

Definitie

Integriteit geeft de mate aan waarin de informatie actueel en correct is. Kenmerken zijn juistheid, volledigheid en tijdigheid van de transacties.

Beveiligingsnormen

Onderstaande tabel beschrijft de beveiligingseisen (en maatregelen) per classificatieniveau, onderverdeeld in eisen voor authenticatie, autorisatie, monitoring en beveiliging. De bewaartermijnen zijn indicatief. Voor gegevens waarin (herleidbare) persoonsgegevens voorkomen moet boven de 6 maanden bewaartermijn formeel melding gedaan worden bij de privacy functionaris of het agentschap BPR.

Niveau	Authenticatie	Autorisatie	Monitoring	Beveiliging
Niet zeker	Geen	Geen	Geen	Geen
Beschermd	Authenticatie 'basis' vereist.	Autorisatie vereist.	Vastleggen authenticatie (correct en foutief) en tijdstip. Vastleggen relevante input en output van een IT-systeem of service. Monitoring-gegevens bewaren voor periode van 1/2 jaar. ⁵	Inputvalidatie. Controleren op mutatie tijdens transport. Transportbeveiliging of berichtbeveiliging. Gegevens: Versie van gebruikte gegevens is bekend. ^{6,7} Na uitvoering van een service blijven gewijzigde gegevens consistent.
Hoog	Authenticatie 'midden' vereist.	Autorisatie vereist. 4-ogen principe vereist.	Vastleggen authenticatie (correct en foutief) en tijdstip. Vastleggen relevante input en output van een IT-systeem of service. Monitoring-gegevens bewaren voor periode van maximaal 2 jaar of langer bij een vermoed beveiligingsincident.	Inputvalidatie. Controleren op mutatie tijdens transport. Berichtbeveiliging. Gegevens: Versie van gebruikte gegevens is bekend. Wijzigingen alleen op bron. Na uitvoering van een service blijven gewijzigde gegevens consistent.
Absoluut	Authenticatie 'hoog' vereist. Geen SSO toegestaan.	Autorisatie vereist. 4-ogen principe vereist.	Vastleggen authenticatie (correct en foutief) en tijdstip. Vastleggen relevante input en output van een IT-systeem of service. Monitoring-gegevens bewaren voor periode van minimaal 3 ⁸ jaar bij een vermoed beveiligingsincident. Vastleggen oude staat van te wijzigen gegevens.	Inputvalidatie. Controleren op mutatie tijdens transport. Berichtbeveiliging. Gegevens: Gegevens worden niet buiten hun bron opgeslagen (behalve voor beschikbaarheid~) en niet buiten hun bron gewijzigd. Na uitvoering van een service blijven gewijzigde gegevens consistent.

De authenticatieniveaus verwijzen naar het vereiste beveiligingsmechanisme:

- Basis: authenticatie gebaseerd op iets wat men weet (naam/wachtwoord).
- Midden: authenticatie gebaseerd op iets wat men weet en iets wat men heeft (bijv. een token, smartcard of certificaat).

⁵ Voor zover niet in strijd met wetgeving wat betreft de vastlegging van gegevens.

⁶ Het gaat om de bron van de gegevens of een kopie van de gegevens en het tijdstip van de gebruikte gegevens.

⁷ Regels met betrekking tot gegevensuitwisseling met derden (buiten Gemeente XXXXXXXXX) worden gedefinieerd in een leveringscontract. Hierin komen ook regels met betrekking tot integriteit en vertrouwelijkheid aan bod

⁸ Zie 10.10.3.5 van de tactische variant van de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG).

- Hoog: authenticatie gebaseerd op eigenschap, bijvoorbeeld irisscan of vingerafdruk. De autorisatieniveaus verwijzen naar de wijze waarop de controle wordt uitgevoerd. Vanaf beschermd is altijd autorisatie verplicht en vanaf hoog komt daar het 4-ogen principe bij. Het 4-ogen principe bestaat uit één persoon die vastlegt en één persoon die fiatteert.

Bij monitoring van de niveaus 'beschermd' en 'hoog' wordt de term 'relevant' gebruikt. Welke gegevens 'relevant' zijn, is ter beoordeling van de eigenaar. Voorbeelden en richtlijnen voor relevante gegevens zijn stamgegevens (gegevens waarop andere gegevens gebaseerd zijn), gegevens in basis- en kernregistraties, privacygevoelige informatie en gegevens beschermd door wet- en regelgeving.

Bij datatransport is berichtbeveiliging te prefereren boven transportbeveiliging. Echter, transportbeveiliging kan in bepaalde gevallen eenvoudiger en/of goedkoper te implementeren zijn. Daarom is bij classificatieniveau 'beschermd' de keuze voor transportbeveiliging en berichtbeveiliging open gelaten. Bij 'hoog' en 'absoluut' is de classificatie zodanig dat berichtbeveiliging toegepast moet worden.

5.3 Vertrouwelijkheid

Definitie

Vertrouwelijkheid is het kwaliteitsbegrip waaronder privacybescherming maar ook de exclusiviteit van informatie gevangen kan worden. Het waarborgt dat alleen geautoriseerden toegang krijgen en dat informatie niet kan uitlekken.

Vertrouwelijkheid geeft de mate aan waarin de informatie actueel en correct is. Kenmerken zijn juistheid, volledigheid en geautoriseerdheid van de transacties

Vertrouwelijke gegevens zijn bijvoorbeeld:

- Persoonsgegevens
- Gemeentelijke- en bedrijfsgeheimen
- Concurrentiegevoelige gegevens zoals voorbereidingen voor bestemmingsplannen
- Medische gegevens

Beveiligingsmaatregelen

Onderstaande tabel beschrijft de beveiligingseisen (en maatregelen) per classificatieniveau, onderverdeeld in eisen voor authenticatie, autorisatie, monitoring en beveiliging.

Niveau	Authenticatie	Autorisatie	Monitoring	Beveiliging
Openbaar	Geen	Geen	Geen	Geen
Bedrijfs- vertrouwelijk	Authenticatie 'basis' vereist. Sessie-timeout na 15 min inactiviteit. Voor klant absolute sessie-timeout na 120 min. Identiteit blokkeren na 3 achtereenvolgende foutieve authenticatiepogingen. Authenticatie 'basis' nodig voor deblokkeren.	Autorisatie vereist (lid van organisatie).	Vastleggen herhaaldelijk foutieve authenticatie en tijdstip. ⁹ Monitoring-gegevens bewaren voor periode van 1/2 jaar.	Outputvalidatie. Versleuteling tijdens transport buiten netwerk van Gemeente <gemeentenaam> via transportbeveiliging of berichtbeveiliging. Kopieën van gegevens moeten net zo goed beveiligd worden. Gegevens uit productieomgeving worden niet gebruikt in OTA ¹⁰ -omgevingen tenzij deze zijn geanonimiseerd en de geveenseigenaar toestemming heeft gegeven.
Vertrouwelijk	Authenticatie 'midden' vereist. Sessie-timeout na 15 min inactiviteit. Voor klant absolute sessie-timeout na 120 min. Identiteit blokkeren na 3 achtereenvolgende foutieve authenticatiepogingen. Authenticatie 'midden' nodig voor deblokkeren.	Autorisatie vereist (specifieke rol).	Vastleggen herhaaldelijk foutieve authenticatie en tijdstip. Monitoring-gegevens bewaren voor periode van 2 jaar.	Outputvalidatie. Versleuteling tijdens transport en op tussenstations binnen en buiten netwerk van Gemeente <gemeentenaam> via berichtbeveiliging. Kopieën van gegevens moeten minimaal net zo goed beveiligd worden. Aantal kopieën minimaliseren. Berichtbeveiliging. Gegevens uit productieomgeving worden niet gebruikt in OTA-omgevingen tenzij deze zijn geanonimiseerd en de geveenseigenaar toestemming heeft gegeven.
Geheim	Authenticatie 'hoog' vereist. Sessie-timeout na 15 min inactiviteit. Voor klant absolute sessie-timeout na 120 min. Identiteit blokkeren na 3 achtereenvolgende foutieve authenticatiepogingen. Authenticatie 'hoog' nodig voor deblokkeren. Geen SSO toegestaan.	Autorisatie vereist (specifieke rol).	Vastleggen correcte en foutieve authenticatie en tijdstip. Monitoring-gegevens bewaren voor periode van 7 jaar.	Outputvalidatie. Versleuteling tijdens transport en op tussenstations via berichtbeveiliging. Versleutelde opslag van gegevens. Transport van gegevens minimaliseren. Alleen transport en opslag binnen vaste netwerk van Gemeente <gemeentenaam>. Geen kopieën toegestaan behalve voor beschikbaarheid. Gegevens uit productieomgeving worden niet gebruikt in OTA-omgevingen tenzij deze zijn geanonimiseerd en de geveenseigenaar toestemming heeft gegeven.

De authenticatie niveaus verwijzen naar het vereiste beveiligingsmechanisme (zie voorgaande paragraaf). Bedrijfsvertrouwelijk verwijst naar de 'organisatie', waarmee wordt bedoeld: de Gemeente <gemeentenaam>, een deelgemeente of een dienst.

⁹ Onder 'herhaaldelijk foutief' wordt in de context van monitoring gesproken als een identiteit achtereenvolgens drie keer foutief authenticceert. Na correct inloggen wordt de teller 'op nul gezet'.

¹⁰ Ontwikkel-, Test- en Acceptatie- omgevingen

6 Bepalen van classificatieniveaus

In de voorgaande hoofdstukken is de context beschreven die van belang is bij het toekennen van classificatieniveaus: de beleidsuitgangspunten, architectuurprincipes en beveiligingseisen. Met deze kennis kan data geclassificeerd gaan worden. In dit hoofdstuk zijn de te doorlopen stappen uitgewerkt.

Stap 1: Wettelijke eisen

De eerste stap bij dataclassificatie is nagaan welke wet en regelgeving mogelijk eisen stelt aan gebruik, distributie en opslag van data.

Zie voor een overzicht van relevante wetgeving hoofdstuk 1.5 van de tactische variant van de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG).

Vooraf in de Wet Bescherming Persoonsgegevens (WBP) worden eisen gesteld aan de verwerking van persoonsgegevens, waarbij het begrip 'passende beveiligingsmaatregelen' een rol speelt. De WBP bepaalt dat persoonsgegevens door de verantwoordelijke (degene die doel en middelen van de verwerking vaststelt) in overeenstemming met de wet en op behoorlijke en zorgvuldige wijze dienen te worden verwerkt (artikel 6 WBP). Tevens dienen persoonsgegevens voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden te worden verzameld (artikel 7 WBP). Ook mogen persoonsgegevens niet verder worden verwerkt op een wijze die onverenigbaar is met de doeleinden waarvoor ze zijn verkregen (artikel 9 WBP). Daarnaast dienen persoonsgegevens die worden verwerkt toereikend, ter zake dienend, niet bovenmatig, juist en nauwkeurig te zijn (artikel 11 WBP). Deze bepalingen zijn leidend bij de toekenning van classificatieniveaus.

Het beschermingsniveau van data is veelal het resultaat van een afweging van belangen. Bijvoorbeeld, het verstrekken van informatie volgens de WOB dient achterwege te blijven voor zover het belang daarvan niet opweegt tegen bijvoorbeeld inspectie, controle en toezicht door bestuursorganen (WOB, art 10, 2d). Voor een zorgvuldige afweging van wat wel/niet toegestaan is, is het raadzaam een jurist of een juridische dienst in te schakelen.

Stap 2: Verantwoordelijkheden t.a.v. data

Voor het toekennen van classificatieniveaus is het van belang om verantwoordelijkheden t.a.v. data en/of informatiesystemen goed in beeld te hebben:

- Wie bepaalt wie data mag gebruiken? Wie is bevoegd het beschermingsniveau te bepalen (rekening houdend met doelbinding in de wetgeving)?
- Wie heeft een 'business' belang bij gebruik van deze data? NB: de eigenaar van de data is niet per definitie de grootste belanghebbende. Houd hier rekening mee bij het bepalen van het classificatieniveau.
- Bepaal wie er allemaal gebruik maakt van data en/of informatiesystemen en welke rechten zij hebben. NB: dit is relevant bij het bepalen van risico's. Data die slechts voor enkelen toegankelijk is, is minder kwetsbaar dan data die breed wordt gedistribueerd via bijvoorbeeld een datawarehouse t.b.v. bedrijfsapplicaties.

Hoewel de eigenaar van de gegevens verantwoordelijk is voor classificatie zal kennis over gebruik, distributie en opslag én kennis van de beveiligingscontext veelal bij anderen liggen. Bij het

classificeren kan de eigenaar van de gegevens de hulp inroepen van de verantwoordelijk functioneel beheerder en de persoon die belast is met de rol van informatiebeveiligingsfunctionaris of CISO.

Stap 3: Analyse kritische bedrijfsprocessen

Classificatieniveaus zijn afgeleid van de waarde van data en het belang van het bedrijfsproces waarin deze data een rol speelt. Stel daarom vast wat het belang is van de bedrijfsvoerings processen voor de organisatie en hoe deze processen worden ondersteund door de ICT voorzieningen.

De analyse wordt uitgevoerd met de modelvragenlijsten uit bijlage 1. Deze vragenlijsten geven direct het gewenste classificatieniveau voor beschikbaarheid, integriteit en/of vertrouwelijkheid van een informatiebedrijfsmiddel.

In het kader van reproduceerbaarheid en voor bijvoorbeeld auditpartijen die achtergrond gegevens vragen, maar ook om vergelijkingen mogelijk te maken bij toekomstige herclassificatie, sterk aanbevolen om de ingevulde vragenlijsten te archiveren.

In 2007 heeft de voorloper van het NCSC, GovCert, een onderzoek uitgevoerd met een aantal gemeenten, naar de betrouwbaarheidseisen voor een aantal uitvoeringsprocessen. Deze staan in onderstaande tabel en zijn bedoeld als leidraad.

Proces	Beschikbaarheid	Integriteit	Vertrouwelijkheid
Burgerzaken (klantbegeleiding, afspraken)	Belangrijk	Absoluut	Vertrouwelijk
Basisregistratie persoonsgegevens	Essentieel	Absoluut	Geheim
Overige basisregistraties	Essentieel	Absoluut	Openbaar
Indienen en behandelen beroep en bezwaarschriften	Noodzakelijk	Absoluut	Openbaar/ vertrouwelijk
Registratie ingekomen post burgers en bedrijven	Noodzakelijk	Hoog	Bedrijfsvertrouwelijk
Beheren gevonden voorwerpen	Noodzakelijk	Beschermd	Openbaar
Bedrijvenloket	Noodzakelijk	Beschermd	Openbaar
Publicatie van ruimtelijke plannen	Noodzakelijk	Absoluut	Openbaar
Grootschalige Basiskaart Nederland (GBKN)	Noodzakelijk	Absoluut	Openbaar
Kenbaarstelling Publiekrechtelijke Beperkingen (WKPB)	Noodzakelijk	Absoluut	Openbaar
Registratie risico's gevaarlijke stoffen (risicokaart)	Essentieel	Absoluut	Bedrijfsvertrouwelijk
Bodembeheer	Noodzakelijk	Hoog	Openbaar
Aanvraag en verlening vergunning	Noodzakelijk	Absoluut	Vertrouwelijk
Bouw- en woningtoezicht	Noodzakelijk	Absoluut	Vertrouwelijk
Financieel beheer (betalingen leges, etc.)	Noodzakelijk	Hoog	Vertrouwelijk
Aangifte en heffing gemeentelijke belastingen/ heffingen	Noodzakelijk	Hoog	Vertrouwelijk
Waardebepaling Onroerende Zaken (W OZ)	Noodzakelijk	Hoog	Bedrijfsvertrouwelijk
Sociale Zaken — Uitvoering / verstrekking voorzieningen	Essentieel	Hoog	Geheim
Sociale Zaken — Handhaving en controle	Noodzakelijk	Absoluut	Geheim

Openbare orde en veiligheid (brandweer, preventie,	Essentieel	Absoluut	Geheim
Handhaving en toezicht gemeentelijke verordeningen /	Noodzakelijk	Absoluut	Vertrouwelijk
Gezondheidszorg – GGD taak / ambulancedienst	Belangrijk	Absoluut	Geheim

Stap 4: Afweging: criteria bij het bepalen van het classificatieniveau

Classificeren is geen exacte wetenschap. Bepaling van het classificatieniveau volgt uit een risicobeoordeling waarin de 'waarde' van informatie wordt bepaald. Aangezien 'waarde' lang niet altijd meetbaar is, is toekenning van een classificatieniveau soms arbitrair. In die gevallen kan een afweging gemaakt worden tussen de waarde en het risico van verlies van data. Het classificatieniveau en de daarbij behorende beveiligingseisen en maatregelen moet altijd 'passen' bij het te beschermen gegeven. De vraag is natuurlijk: wat is een 'passende' maatregel?

Artikel 13 WBP noemt drie criteria die bij de keuze van de te nemen technische en organisatorische maatregelen gebruikt moeten worden:

1. De stand der techniek
 - Hierbij wordt allereerst vastgesteld welke technische maatregelen op dat moment beschikbaar zijn;
 - Ten aanzien van de aanwezige voorzieningen geldt dat achterhaalde technieken niet langer als passend geclassificeerd kunnen worden;
 - Dit betekent dat een verantwoordelijke bij het bepalen van de te nemen technische maatregelen een afstemming moet vinden tussen de technische faciliteiten die in gebruik zijn bij de verwerking en die in gebruik zijn bij de beveiliging van persoonsgegevens;
 - De verantwoordelijke moet deze analyse periodiek herhalen.
2. De kosten van de tenuitvoerlegging
 - Hier moet de verantwoordelijke een keuze maken tussen de mogelijke technische en organisatorische maatregelen: in alle redelijkheid moet worden afgewogen of er een evenredigheid bestaat tussen de kosten van de beveiliging en het effect daarvan voor de beveiliging van persoonsgegevens;
3. De risico's die de verwerking met zich meebrengen
 - Hier wordt vastgesteld welk risico de betrokkene c.q. De verantwoordelijke lopen bij verlies of onrechtmatige verwerking van persoonsgegevens: naarmate het risico toeneemt zullen de maatregelen evenredig verzaamd worden.

Classificeren kan het beste in workshopverband uitgevoerd worden. Een workshop heeft een lerend effect, geeft commitment binnen de groep, zorgt voor samenwerken, maar bovenal zorgt het voor een gewogen gemiddelde. Dit laatste heeft als resultaat dat maatregelen beter in perspectief komen.

Stap 5: Het resultaat

Het resultaat van de analyse vertaald zich in een classificatierapport met daarbij de ingevulde vragenlijsten als bijlagen.

Het beveiligingsniveau van de Tactische Baseline is zo gekozen dat dit voor de meeste processen en ondersteunende ICT-voorzieningen bij gemeenten voldoende is. Hiermee wordt voorkomen dat er voor ieder systeem een uitgebreide risicoanalyse uitgevoerd moet worden.

Het niveau van de Baseline Informatiebeveiliging Nederlandse Gemeenten bevindt zich op de volgende (BIV) waarden:

- Beschikbaarheid: Noodzakelijk
- Integriteit: Hoog
- Vertrouwelijkheid: Vertrouwelijk

Mocht de uitkomst van de analyse uitkomen onder of op de bovenstaande niveaus, dan hoeven geen extra maatregelen genomen te worden. Als één van de BIV-waarden een hogere score heeft dan hierboven genoemd, dan moeten er extra maatregelen genomen worden. Deze maatregelen worden separaat beschikbaar gesteld als aanvullende maatregelen al naar gelang de behaalde BIV-score.

Bijlage 1: Classificatie leidraad

Het classificatieproces bij <naam gemeente> wordt ondersteund door een drietal vragenlijsten, waarmee de impact op het bedrijfsproces wordt bepaald:

- a. Vragen over beschikbaarheid
- b. Vragen over integriteit
- c. Vragen over vertrouwelijkheid

De impact op het bedrijfsproces wordt beoordeeld op een 5-puntschaal.

Schaalverdeling:

1. Verwaarloosbaar
2. Geringe schade
3. Belangrijke schade
4. Ernstige schade
5. Bedreigt het voortbestaan van de gemeente

Vanuit de impact op de bedrijfsproces beoordelingen (5-puntschaal) kan een vertaling gemaakt worden naar de 3-puntschaal die gebruikt wordt voor de BIV-classificatie.

Voor de classificatie naar de inzichten **integriteit** en **vertrouwelijkheid** is de vertaling als volgt:

Bedrijfsproces impact	I-classificatie	V-classificatie
1	0 - Verwaarloosbaar	0 - Openbaar
2	1 - Beschermd	1 - Bedrijfsvertrouwelijk
3 + 4	2 - Hoog	2 - Vertrouwelijk
5	3 - Absoluut	3 - Geheim

Voor de **beschikbaarheid** is deze verdeling niet zo direct te leggen, maar de impact beoordeling die daar uit komt geeft over het algemeen voldoende aanknopingspunt om een classificatie naar belangrijk, noodzakelijk en essentieel te maken.

Bijlage 2: Classificatie vragenlijsten

Deze bijlage kan als apart invuldocument gebruikt worden en als basis dienen om de classificaties vast te stellen. Vul onderstaande gegevens in.

Document eigenaar	
Functie	
Organisatie onderdeel	
Telefoonnummer	
Laatste datum invullen	

Het resultaat van het onderzoek voor wat betreft de BIV- aspecten voor het proces <procesnaam> van de <naam gemeente> geeft een inschaling op de volgende niveaus:

- a. Beschikbaarheid :
- b. Integriteit :
- c. Vertrouwelijkheid :

Conclusie: Het proces <procesnaam> valt binnen/buiten de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG) en er zijn wel/niet extra maatregelen nodig. Deze maatregelen kunnen al bestaan als vastgestelde aanvulling of er is een uitgebreide risicoanalyse nodig.

Is er een motivatie om af te wijken van de conclusie (door de systeem eigenaar)?:

Indien er een afwijking is: Is het rest risico acceptabel? JA/NEE

Aldus opgemaakt d.d.

Naam Eigenaar

B – Vragenlijst beschikbaarheid

In het kader van beschikbaarheid is het goed te kijken naar hoe groot de schade is die ontstaat bij een bepaalde uitvalduur.

- a. Welke groep gebruikers wordt getroffen door uitval van het informatiebedrijfsmiddel? En hoe groot is die groep? Wat is naar schatting het aantal gelijktijdige gebruikers in het informatiebedrijfsmiddel?
- b. Wat moeten de openstellingstijden voor het informatiebedrijfsmiddel zijn? Welk beschikbaarheidspercentage is dan wenselijk?
- c. Welke frequentie van systeemuitval wordt nog als acceptabel ervaren? (per maand / kwartaal / jaar)
- d. Is er een continuïteitsplan voor het informatiebedrijfsmiddel?
- e. Is er sprake van kritieke uitval momenten? (denk bijv. aan salarisadministratie aan het eind van de maand, peildatum rapportages, verkiezingen, openingstijden, calamiteiten)
- f. Maximaal toegestane down time?

Business impact schaalverdeling:

1. Verwaarloosbaar
2. Geringe schade
3. Belangrijke schade
4. Ernstige schade
5. Bedreigt het voortbestaan van de gemeente

Business consequentie	Business impact				
	uur	dag	week	2-3 weken	maand
Wanneer maximale schade?					
Management beslissingen Hoe schadelijk is het als op basis van niet beschikbaarheid, verkeerde management beslissingen worden genomen?					
Direct verlies inkomsten Verliezen we inkomsten als de bedrijfsinformatie niet beschikbaar is?					
Publiek vertrouwen Wordt het vertrouwen geschaad of is er imagoschade als informatiebedrijfsmiddel niet beschikbaar is?					
Extra kosten Moeten er extra kosten gemaakt worden als het informatiebedrijfsmiddel niet beschikbaar is?					
Aansprakelijkheid Kan het niet beschikbaar zijn van een applicatie leiden tot enige vorm van aansprakelijkheid?					
Recovery Wat kost het om de achterstand in werk weer weg te werken na een herstart?					
Medewerkers moreel Heeft het nadelige effecten voor het moreel of de motivatie van gebruikers als die applicatie niet beschikbaar is?					
Fraude Kan niet beschikbaar zijn van informatiebedrijfsmiddel leiden tot frauduleuze handelingen?					
Totaalscore In samenvatting: wat de meest ernstige schade is die kan optreden bij uitval op het meest kritische moment?					

I – Vragenlijst integriteit

In het kader van integriteit is het van belang te beoordelen wat de gevolgen kunnen zijn van fouten in gegevens. Dit geldt zowel voor opzettelijke fouten (of fraude) als onopzettelijke fouten.

Gaat het bij vertrouwelijkheid om de vraag of een ander het gegeven mag zien, bij integriteit gaat het erom of de ander het gegeven mag muteren. Kernbegrippen zijn juistheid en volledigheid.

- a. Vormen de gegevens in het informatiemiddel de basis voor management beslissingen?
- b. Welke bewaartermijnen zijn van toepassing? (archiefwet, WBP, fiscale wetgeving,...)
- c. Wordt er systematisch gecontroleerd op juistheid en volledigheid?
- d. Vanaf welk soort werkplekken moeten gegevens beschikbaar zijn? (altijd en overal, thuis, onderwijslokalen, personeelswerkplek)
- e. Kan een gebruiker onrechtmatig voordeel behalen door een gegeven opzettelijk te veranderen? (fraude te plegen)
- f. Maximaal toegestaan dataverlies na uitval?

Business impact schaalverdeling:

1. Verwaarloosbaar
2. Geringe schade
3. Belangrijke schade
4. Ernstige schade
5. Bedreigt het voortbestaan van de gemeente

Business consequentie	Business impact				
Wanneer maximale schade?	1	2	3	4	5
Management beslissingen Hoe schadelijk is het als op basis van deze informatie verkeerde management beslissingen worden genomen?					
Direct verlies inkomsten Verliezen we inkomsten als informatie ongeautoriseerd gewijzigd wordt?					
Publiek vertrouwen Hoe groot is de imagoschade als onjuiste informatie wordt gebruikt?					
Aansprakelijkheid Kan onjuistheid van gegevens leiden tot enige vorm van aansprakelijkheid?					
Medewerkers moreel Heeft het nadelige effecten voor het moreel of de motivatie van gebruikers als ze met onjuiste informatie moeten werken?					
Fraude Welke impact hebben frauduleuze handelingen?					
Totaalscore In samenvatting: gegeven de bovenstaande scores (en eventueel andere consequenties) wat is dan de grootste schade die kan ontstaan door fouten of ongeautoriseerde wijzigingen? (dit zou normaal minimaal gelijk moeten zijn aan de grootste schade op individuele basis)					

V – Vragenlijst vertrouwelijkheid

Om te bepalen óf en hoe vertrouwelijk informatie is, is het van belang te weten wat de business consequenties zijn van ongeplande of ongeautoriseerde openbaarmaking of bekend worden van die informatie. Een speciale categorie vertrouwelijke gegevens zijn de persoonsgegevens. Bij de verwerking hiervan hebben we ons te houden aan de Wet Bescherming Persoonsgegevens. Deze laat veel toe maar stelt wel voorwaarden aan de verwerking en dan vooral aan de zorgvuldigheid van omgang met die gegevens.

- a. Worden in het informatiebedrijfsmiddel gegevens opgeslagen of verwerkt welke herleidbaar zijn tot natuurlijke personen?
- b. Bevat het systeem bijzonder persoonsgegevens als bedoelt in de WBP art. 16?
- c. Bevat het informatiebedrijfsmiddel informatie die gecombineerd met informatie uit andere systemen herleidbaar is tot natuurlijke personen?
- d. Bevat het informatiebedrijfsmiddel concurrentiegevoelige gegevens (bijv. tarievenopbouw, contracten)?
- e. Bevat het informatiebedrijfsmiddel informatie onder embargo?
- f. Bevat het informatiemiddel informatie die alleen voor een specifieke doelgroep beschikbaar mag zijn? (denk ook aan licentiebeperingen)
- g. Bevat het informatiebedrijfsmiddel gegevens die gebruikt kunnen worden om fraude te plegen? (denk bijv. aan identiteitsfraude, creditcardnummers, wachtwoordbestanden).

Business impact schaalverdeling:

1. Verwaarloosbaar
2. Geringe schade
3. Belangrijke schade
4. Ernstige schade
5. Bedreigt het voortbestaan van de gemeente

Business consequentie	Business impact				
Wanneer maximale schade?	1	2	3	4	5
Direct verlies inkomsten Verliezen we inkomsten als informatie in verkeerde handen terecht komt?					
Publiek vertrouwen Hoe groot is de imagoschade als deze informatie publiek wordt, hoe groot zijn de nadelige gevolgen voor het vertrouwen dat onze burgers in ons hebben?					
Wetgeving Bevat het systeem persoonsgegevens in de zin van de WBP art 16? ¹¹					
Aansprakelijkheid Kan openbaar maken leiden tot aansprakelijkheidstelling op basis van wettelijke of contractuele verplichtingen?					
Medewerkers moreel Heeft openbaarmaking nadelige effecten op het moreel of de motivatie van medewerkers?					
Fraude Welke impact hebben frauduleuze handelingen t.g.v. bekend worden van deze gegevens?					
Totaalscore In samenvatting: gegeven de bovenstaande scores (en eventueel andere consequenties) wat is dan de grootste schade die kan ontstaan door het onbedoeld of ongeautoriseerde toegang bieden tot deze informatie? (dit zou normaal minimaal gelijk moeten zijn aan de grootste schade op individuele basis)					

¹¹ De verwerking van persoonsgegevens betreffende iemands godsdienst of levensovertuiging, ras, politieke gezindheid, gezondheid, seksuele leven, alsmede persoonsgegevens betreffende het lidmaatschap van een vakvereniging is verboden behoudens het bepaalde in deze paragraaf. Hetzelfde geldt voor strafrechtelijke persoonsgegevens en persoonsgegevens over onrechtmatig of hinderlijk gedrag in verband met een opgelegd verbod naar aanleiding van dat gedrag.

Bijlage 3: Waarderingschaal

De in deze bijlage opgenomen waarderingschaal voor schade is vastgesteld door een middelgrote gemeente. Gemeenten dienen zelf vast te stellen of de hieronder genoemde schade niveaus voor hun van toepassing zijn en indien nodig aan te passen.

	Persoons- informatie	Wettelijke en reglementaire verplichtingen	Financieel verlies	Beleid en werking van de gemeentelijke overheid	Verlies van goodwill
Enige schade Business impact=2	Ongemak voor een persoon, maar er wordt geen inbreuk gemaakt op een wet of op regelgeving.	Civiele procedure of strafrechtelijke vervolging, resulterend in een schadevergoeding /boete van minder dan € 5.000.	Resulteert direct of indirect in verliezen van minder dan € 10.000.	Draagt bij aan het niet efficiënt opereren van een deel van de organisatie.	Heeft een negatieve invloed op de betrekkingen met andere delen van de organisatie of het publiek.
Serieuze schade Business impact=3 of 4	Een inbreuk op wet- of regelgeving, resulterend in licht ongemak voor een persoon of groep personen.	Civiele procedure of strafrechtelijke vervolging, resulterend in een schadevergoeding /boete tussen € 5.000 en € 50.000.	Resulteert direct of indirect in verliezen tussen € 10.000 en € 100.000.	Benadeelt het goed besturen en/of functioneren van een deel van de organisatie.	Heeft een negatieve invloed op de betrekkingen met andere organisaties of het publiek, resulterend in plaatselijke negatieve publiciteit.
Zeer grote schade Business impact=5	Een inbreuk op wet- of regelgeving, resulterend in aanzienlijk ongemak voor een persoon of groep personen.	Civiele procedure of strafrechtelijke vervolging, resulterend in een schadevergoeding /boete boven € 50.000 of een gevangenisstraf.	Resulteert direct of indirect in verliezen boven € 100.000.	Benadeelt het goed besturen en/of functioneren van de gehele organisatie.	Heeft een significante invloed op de betrekkingen met andere organisaties of het publiek, resulterend in wijdverspreide negatieve publiciteit.

INFORMATIE BEVEILIGINGS DIENST

|

**INFORMATIEBEVEILIGINGSDIENST
VOOR GEMEENTEN (IBD)**

**NASSAULAAN 12
2514 JS DEN HAAG**

**POSTBUS 30435
2500 GK DEN HAAG**

**HELPDESK 070 373 80 11
ALGEMEEN 070 373 80 08
FAX 070 363 56 82**

**IBD@KINGGEMEENTEN.NL
WWW.KINGGEMEENTEN.NL**