INFORMATIE
BEVEILIGINGS
DIENST

HANDREIKING DATACLASSIFICATIE

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

KWALITEITSINSTITUUT NEDERLANDSE GEMEENTEN **IN OPDRACHT VAN**
VERENIGING VAN NEDERLANDSE GEMEENTEN

INFORMATIE
BEVEILIGINGS
DIENST

Colofon

Naam document
Handreiking Dataclassificatie

Versienummer
1.6.1

Versiedatum
Augustus 2016

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

Copyright
© 2016 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 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.

Wijzigingshistorie:

versie	datum	Opmerkingen
1	18-10-2013	Eerste versie
1.1	03-11-2014	
1.2	21-07-2014	
1.3	03-30-2015	Foute definitie vertrouwelijkheid bij paragraaf 5.3 verwijderd
1.5	11-03-2016	Waardering gelijk getrokken met baselinetoets BIG Aanpassingen in verband met Meldplicht Datalekken (Wbp) en consistent gemaakt met de Baselinetoets BIG
1.6	27-05-2016	Aanscherping op vallen college in plaats van voortbestaan gemeente
1.6.1	Augustus 2016	Taskforce BID verwijderd

KWALITEITSINSTITUUT NEDERLANDSE GEMEENTEN IN OPDRACHT VAN VERENIGING VAN NEDERLANDSE GEMEENTEN

INFORMATIE
BEVEILIGINGS
DIENST

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 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: BRP, SUWI, BAG, PUN en Wbp, 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.

KWALITEITSINSTITUUT NEDERLANDSE GEMEENTEN IN OPDRACHT VAN VERENIGING VAN NEDERLANDSE GEMEENTEN

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
- Baselinetoets BIG
- Privacy Impact Assessment (PIA) gemeenten
- Diepgaande Risicoanalysemethode gemeenten
- GAP-analyse

Maatregelen tactische variant Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG)
7.2 Informatie behoort te worden geclassificeerd om bij het verwerken van de informatie de noodzaak, prioriteiten en verwachte graad van bescherming te kunnen aangeven.

KWALITEITSINSTITUUT NEDERLANDSE GEMEENTEN IN OPDRACHT VAN VERENIGING VAN NEDERLANDSE GEMEENTEN

Inhoud

KWALITEITSINSTITUUT NEDERLANDSE GEMEENTEN IN OPDRACHT VAN VERENIGING VAN NEDERLANDSE GEMEENTEN

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.

KWALITEITSINSTITUUT NEDERLANDSE GEMEENTEN IN OPDRACHT VAN VERENIGING VAN NEDERLANDSE GEMEENTEN

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.

2.2 Privacy Impact Assessment

Een bijzondere categorie van data zijn persoonsgegevens. Bij persoonsgegevens gaat het om alle informatie over een persoon. Ook gegevens die indirect iets over iemand zeggen, zijn persoonsgegevens. De Wet bescherming persoonsgegevens (Wbp) geeft aan dat een persoonsgegeven elk gegeven is over een geïdentificeerde of identificeerbare natuurlijke persoon. Dit betekent dat informatie ofwel direct over iemand gaat, ofwel naar deze persoon te herleiden is. Dat het om een natuurlijke persoon moet gaan, houdt in dat gegevens van overleden personen of van organisaties geen persoonsgegevens zijn.
Wilt u als gemeente privacyrisico's van een project in een vroeg stadium op een gestructureerde en heldere manier in beeld brengen? Dan kunt u een Privacy Impact Assessment (PIA) (laten) uitvoeren. De PIA legt in de eerste plaats de risico's bloot van projecten die te maken hebben met privacy en dragen bij aan het vermijden of verminderen van deze privacyrisico's.[1]
Op basis van de antwoorden van de PIA wordt op systematische wijze inzichtelijk gemaakt of er een kans is dat de privacy van betrokkene wordt geschaad, hoe hoog deze is en op welke gebieden dit is.

De PIA doet dit door op gestructureerde wijze:
- de mogelijk (negatieve) gevolgen van het gebruik van persoonsgegevens voor de betrokken personen en organisaties in kaart te brengen; en
- de risico's voor de betrokken personen en organisaties zo veel mogelijk te lokaliseren.

Op basis van de uitkomsten van de PIA kunt u gericht acties ondernemen om deze risico's te verminderen. De PIA is een verplicht instrument en een onmisbaar hulpmiddel voor organisaties om de privacyimpact van hun projecten te evalueren. Door het gebruik van de PIA kan bescherming van persoonsgegevens op een gestructureerde manier onderdeel uitmaken van de belangenafweging en besluitvorming over een project.

Is er sprake van het verwerken van een wettelijk identificatienummer (1) of bijzondere persoonsgegevens (2) in de zin van artikel 16 Wbp (godsdienst, levensovertuiging, ras, politieke gezindheid, gezondheid, seksuele leven, lidmaatschap vakvereniging of strafrechtelijke persoonsgegevens of over onrechtmatig of hinderlijk gedrag) en is niet op voorhand helder of er ad 1) sprake van een wettelijk doel of is het niet ter uitvoering van de betreffende wet of ad 2) is niet op

[1] Zie hiervoor het operationele BIG document 'Toelichting PIA' van de IBD.

KWALITEITSINSTITUUT NEDERLANDSE GEMEENTEN IN OPDRACHT VAN VERENIGING VAN NEDERLANDSE GEMEENTEN

voorhand helder dat er sprake van een wettelijke ontheffing van het verwerkingsverbod is dan wel (3) gaat het om een verwerking van persoonsgegevens in een complexe keten.

Meldplicht Datalekken

Alle bedrijven en overheden die persoonsgegevens verwerken op grond van de Wet bescherming persoonsgegevens (Wbp) zijn vanaf 1 januari 2016 verplicht om een ernstig datalek direct te melden aan de Autoriteit Persoonsgegevens (AP), voorheen het College bescherming persoonsgegevens (CBP).[2] De AP heeft beleidsregels over deze nieuwe Meldplicht Datalekken gepubliceerd.[3]
De Meldplicht Datalekken richt zich tot de verantwoordelijke voor de verwerking van persoonsgegevens. De verantwoordelijke is degene die uiteindelijk bepaalt welke verwerking er plaatsvindt van welke persoonsgegevens en voor welk doel. Ook is van belang wie er beslist over de middelen voor die verwerking, de vraag is: op welke manier de gegevensverwerking zal plaatsvinden? De gemeente is in deze situatie altijd de eindverantwoordelijke in de context van de Wbp.
Indien er sprake is van een ernstig datalek, waarbij kans is op verlies of onrechtmatige verwerking van persoonsgegevens, dient de verantwoordelijke het datalek te melden aan de AP. In een aantal gevallen dient het datalek ook gemeld te worden aan de betrokkene. Als er geen melding wordt gemaakt van een datalek kan de AP dit bestraffen met een bestuurlijke boete van maximaal € 820.000. Organisaties kunnen de beleidsregels Meldplicht Datalekken van het AP gebruiken bij het bepalen of er sprake is van een datalek dat moet worden gemeld bij de AP en eventueel aan de betrokkene.
Van belang zijn hierbij onderstaande vragen:

- Zijn doeltreffende maatregelen getroffen waardoor een daadwerkelijke identificatie van individuele natuurlijke personen redelijkerwijs wordt uitgesloten?
- Zijn passende maatregelen getroffen waardoor de persoonsgegevens zijn beschermd tegen onbevoegde kennisname?

Door de AP kan worden getoetst worden of deze baselinetoets BIG is uitgevoerd om vast te stellen of doeltreffende en passende maatregelen zijn genomen.

[2] Zie hiervoor ook de leaflet 'Meldplicht Datalekken' van de IBD.
[3] https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/beleidsregels_meldplicht_datalekken.pdf

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 (0): De gegevens kunnen zonder gevolgen langere tijd niet beschikbaar zijn Schending van beschikbaarheid heeft geen gevolgschade.
- Belangrijk (1): 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 enige[4] (in)directe schade toebrengen
- Noodzakelijk (2): 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 serieuze[5] (in)directe schade toebrengen.
- Essentieel (3): 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) grote[6] schade toebrengen.

De onderscheiden niveaus van integriteit zijn:

- Niet zeker (0): Deze informatie mag worden veranderd. Geen extra bescherming van integriteit noodzakelijk. Schending van integriteit heeft geen gevolgschade.
- Beschermd (1): 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 (2): 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 (3): 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 (0): Alle informatie die algemeen toegankelijk is voor een ieder. Er is geen schending van deze classificatie mogelijk.
- Bedrijfsvertrouwelijk (1): 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 (2): Informatie die alleen toegankelijk mag zijn voor een beperkte groep gebruikers[7]. De informatie wordt ter beschikking gesteld op basis van vertrouwen. Schending van deze classificatie kan serieuze (in)directe schade toebrengen.
- Geheim (3): Dit betreft gevoelige informatie die alleen toegankelijk mag zijn voor de direct geadresseerde. Schending van deze classificatie kan zeer grote schade toebrengen.

[4] Voor uitleg over 'enige' zie bijlage 3
[5] Voor uitleg over 'serieuze' zie bijlage 3
[6] Voor uitleg over 'zeer grote' zie bijlage 3
[7] 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.

KWALITEITSINSTITUUT NEDERLANDSE GEMEENTEN IN OPDRACHT VAN VERENIGING VAN NEDERLANDSE GEMEENTEN

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.

KWALITEITSINSTITUUT NEDERLANDSE GEMEENTEN IN OPDRACHT VAN VERENIGING VAN NEDERLANDSE GEMEENTEN

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 Belangrijk		
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 Noodzakelijk		
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.)
MTBF	100 dagen	(min.)

KWALITEITSINSTITUUT NEDERLANDSE GEMEENTEN IN OPDRACHT VAN VERENIGING VAN NEDERLANDSE GEMEENTEN

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.

Beveiligingsmaatregelen

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 de Rijksdienst voor Identiteitsgegevens (RvIG).[8]

[8] Het Agentschap Basisadministratie Persoonsgegevens en Reisdocumenten (BPR) van het ministerie van Binnenlandse Zaken en Koninkrijksrelaties heet vanaf 1 maart 2015 Rijksdienst voor Identiteitsgegevens (RvIG).

KWALITEITSINSTITUUT NEDERLANDSE GEMEENTEN IN OPDRACHT VAN VERENIGING VAN NEDERLANDSE GEMEENTEN

Niveau	Authenticatie	Autorisatie	Monitoring	Beveiliging
Niet zeker (0)	Geen	Geen	Geen	Geen
Beschermd (1)	Authenticatie 'basis' vereist.	Autorisatie vereist.	Vastleggen authenticatie (correct en foutief) en tijdstip. Vastleggen relevante input en output van een ICT-systeem of service. Monitoringsgegevens bewaren voor periode van 1/2 jaar.[9]	Invoervalidatie. Controleren op mutatie tijdens transport. Transportbeveiliging of berichtbeveiliging. Versie van gebruikte gegevens is bekend.[10][11] Na uitvoering van een service blijven gewijzigde gegevens consistent.
Hoog (2)	Authenticatie 'midden' vereist.	Autorisatie vereist. 4-ogen principe vereist.	Vastleggen authenticatie (correct en foutief) en tijdstip. Vastleggen relevante input en output van een ICT-systeem of service. Monitoringsgegevens bewaren voor periode van maximaal 2 jaar of langer bij een vermoed beveiligingsincident.	Invoervalidatie. Controleren op mutatie tijdens transport. Berichtbeveiliging. Versie van gebruikte gegevens is bekend. Wijzigingen alleen op bron. Na uitvoering van een service blijven gewijzigde gegevens consistent.
Absoluut (3)	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 ICT-systeem of service. Monitoringsgegevens bewaren voor periode van minimaal 3 [12]jaar bij een vermoed beveiligingsincident. Vastleggen oude staat van te wijzigen gegevens.	Invoervalidatie. Controleren op mutatie tijdens transport. Berichtbeveiliging. 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 (1 factor): authenticatie gebaseerd op iets wat men weet (naam/wachtwoord).
- Midden (2 factor): authenticatie gebaseerd op iets wat men weet en iets wat men heeft (bijv. een token, smartcard of certificaat).
- Hoog (3 factor): 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

[9] Voor zover niet in strijd met wetgeving wat betreft de vastlegging van gegevens.
[10] Het gaat om de bron van de gegevens of een kopie van de gegevens en het tijdstip van de gebruikte gegevens.
[11] 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
[12] Zie 10.10.3.5 van de tactische variant van de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG).

KWALITEITSINSTITUUT NEDERLANDSE GEMEENTEN IN OPDRACHT VAN VERENIGING VAN NEDERLANDSE GEMEENTEN

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.

Vertrouwelijke gegevens zijn bijvoorbeeld:

- Persoonsgegevens
- Gemeentelijke- en bedrijfsgeheimen
- Concurrentiegevoelige gegevens zoals voorbereidingen voor bestemmingsplannen
- Medische gegevens[13]

Beveiligingsmaatregelen

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

[13] Als de gemeenten medische gegevens nodig heeft om de zorg van een burger goed in kaart te kunnen brengen, dan zal de gemeente aan deze burger dienen te vragen die gegevens te geven. Of de gemeente vraagt aan deze burger om toestemming de medische gegevens op te mogen vragen bij bijvoorbeeld de zorgaanbieder.

Niveau	Authenticatie	Autorisatie	Monitoring	Beveiliging
Openbaar (0)	Geen	Geen	Geen	Geen
Bedrijfs-vertrouwelijk (1)	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.[14] Monitoringsgegevens bewaren voor periode van 1/2 jaar.	Uitvoervalidatie. 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[15]-omgevingen tenzij deze zijn geanonimiseerd en de gegevenseigenaar toestemming heeft gegeven.
Vertrouwelijk (2)	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. Monitoringsgegevens bewaren voor periode van 2 jaar.	Uitvoervalidatie. 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 gegevenseigenaar toestemming heeft gegeven.
Geheim (3)	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. Monitoringsgegevens bewaren voor periode van 7 jaar.	Uitvoervalidatie. 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 gegevenseigenaar 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.

[14] Onder 'herhaaldelijk foutief' wordt in de context van monitoring gesproken als een identiteit achtereenvolgens drie keer foutief authenticeert. Na correct inloggen wordt de teller 'op nul gezet'.
[15] 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).

Vooral 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 Wet openbaarheid van bestuur (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)	Noodzakelijk	Absoluut	Vertrouwelijk
Basisregistratie persoonsgegevens	Essentieel	Absoluut	Geheim
Overige basisregistraties	Essentieel	Absoluut	Openbaar
Indienen en behandelen beroep en bezwaarschriften	Belangrijk	Absoluut	Openbaar/ vertrouwelijk
Registratie ingekomen post burgers en bedrijven	Belangrijk	Hoog	Bedrijfsvertrouwelijk
Beheren gevonden voorwerpen	Belangrijk	Beschermd	Openbaar
Bedrijvenloket	Belangrijk	Beschermd	Openbaar
Publicatie van ruimtelijke plannen	Belangrijk	Absoluut	Openbaar
Grootschalige Basiskaart Nederland (GBKN)	Belangrijk	Absoluut	Openbaar
Kenbaarstelling Publiekrechtelijke Beperkingen (WKPB)	Belangrijk	Absoluut	Openbaar
Registratie risico's gevaarlijke stoffen (risicokaart)	Essentieel	Absoluut	Bedrijfsvertrouwelijk
Bodembeheer	Belangrijk	Hoog	Openbaar
Aanvraag en verlening vergunning	Belangrijk	Absoluut	Vertrouwelijk
Bouw- en woningtoezicht	Belangrijk	Absoluut	Vertrouwelijk
Financieel beheer (betalingen leges, et cetera)	Belangrijk	Hoog	Vertrouwelijk
Aangifte en heffing gemeentelijke belastingen/ heffingen	Belangrijk	Hoog	Vertrouwelijk
Waardebepaling Onroerende Zaken (WOZ)	Belangrijk	Hoog	Bedrijfsvertrouwelijk
Sociale Zaken — Uitvoering / verstrekking voorzieningen	Essentieel	Hoog	Geheim
Sociale Zaken — Handhaving en controle	Belangrijk	Absoluut	Geheim
Openbare orde en veiligheid (brandweer, preventie, rampbestrijding)	Essentieel	Absoluut	Geheim
Handhaving en toezicht gemeentelijke verordeningen / regelgeving	Belangrijk	Absoluut	Vertrouwelijk
Gezondheidszorg — GGD taak / ambulancedienst	Noodzakelijk	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 verzwaard 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 vertaalt 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: Belangrijk (1) - 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 enige[16] (in)directe schade toebrengen

[16] Voor uitleg over 'enige' zie bijlage 3

- Integriteit: Hoog (2) - 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.
- Vertrouwelijkheid: Vertrouwelijk (2) - Informatie die alleen toegankelijk mag zijn voor een beperkte groep gebruikers. [17] De informatie wordt ter beschikking gesteld op basis van vertrouwen. Schending van deze classificatie kan serieuze (in)directe schade toebrengen.

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.

[17] 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.

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 basis van de volgende 4-puntsschaal:

0. Verwaarloosbare schade
1. Belangrijke schade
2. Ernstige schade
3. Bedreigt het voortbestaan van de gemeente

Vanuit de impact op de bedrijfsproces beoordelingen (4-puntsschaal) kan een vertaling gemaakt worden naar de 4-puntsschaal 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
0	0 - Verwaarloosbaar	0 - Openbaar
1	1 – Beschermd	1 - Bedrijfsvertrouwelijk
2	2 – Hoog	2 - Vertrouwelijk
3	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 :

<Gebruik voor een verklaring van de resultaten, de waardes van de BIV waardering, de verklarende toelichting uit hoofdstuk 3 'Beleidskaders voor classificatie' uit dit document. Dat maakt het advies leesbaarder en begrijpelijker voor niet informatiebeveiligers.>

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[18]

Aldus opgemaakt d.d.

Naam Eigenaar

[18] Doorhalen wat niet van toepassingen is.

B – Vragenlijst 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 dienst 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.

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?

<u>Invulinstructie</u>
Bij beschikbaarheid is het van belang om bij verschillende uitvalstermijnen de schade te weten. Daarom dient per regel, dus per beschikbaarheidsvraag, in iedere kolom een schade waarderingscijfer (bijvoorbeeld 0, 1, 2 of 3) te worden aangegeven. Tevens dient hierbij een onderbouwing te worden gegeven waarom gekozen is voor de betreffende waarderingscijfers.

Gevolgen van het niet beschikbaar hebben van de benodigde informatie of gegevens. *(in het ergste geval)*		Waardering *(uur, dag, week, maand)*				Argumentatie *(verplicht invullen)*
		1u	1d	1w	1m	
B1	**Managementbeslissingen:** Hoe lang duurt het, voordat het nemen van beslissingen nadelig beïnvloedt wordt door het ontbreken van informatie?	0-3	0-3	0-3	0-3	
B2	**Imagoverlies** Hoe lang duurt het voordat er sprake is van imagoverlies wanneer informatie niet voorhanden is?	0-3	0-3	0-3	0-3	
B3	**Hapering dienstverlening** Hoe lang kan de applicatie of informatie niet beschikbaar zijn voordat er daadwerkelijk hapering in de dienstverlening aan burgers/bedrijven/ketenpartners ontstaat?	0-3	0-3	0-3	0-3	*<Dataverlies (Recovery-Point Objective (RPO)) en hersteltijd (Recovery-Time Objective (RTO)) zijn doelstellingen die een belangrijke rol spelen bij disaster recovery. Hoeveel dataverlies (RPO) is acceptabel en binnen welke tijdsperiode (RTO) moet de dienstverlening weer hersteld zijn? Deze vraag heeft betrekking op de hersteltijd (RTO). Vraag B7 heeft betrekking op het dataverlies (RPO).>*
B4	**Wettelijke aansprakelijkheid:** Hoe lang kan de applicatie of informatie niet beschikbaar zijn voordat er wettelijke of contractuele verplichtingen niet kunnen worden nagekomen?	0-3	0-3	0-3	0-3	
B5	**Additionele kosten:** Na welke periode zijn additionele kosten voor de organisatie te verwachten, bij het niet beschikbaar zijn van de applicatie of informatie?	0-3	0-3	0-3	0-3	
B6	**Moreel van de medewerkers:** Na welke periode is er sprake van een duidelijk negatieve invloed op het moreel en de motivatie van medewerkers, wanneer de informatievoorziening hapert?	0-3	0-3	0-3	0-3	

KWALITEITSINSTITUUT NEDERLANDSE GEMEENTEN IN OPDRACHT VAN VERENIGING VAN NEDERLANDSE GEMEENTEN

Gevolgen van het niet beschikbaar hebben van de benodigde informatie of gegevens. *(in het ergste geval)*		Waardering *(uur, dag, week, maand)*				Argumentatie *(verplicht invullen)*
		1u	1d	1w	1m	
B7	**Herstel:** Hoe lang mag het herstellen na een onbeschikbaarheid van een applicatie of informatie duren voordat er daadwerkelijk hapering in de dienstverlening aan burgers/bedrijven/ketenpartners ontstaat? Zijn er hoge herstelkosten? Dus achteraf verwerken van verloren gegaan werk.	0-3	0-3	0-3	0-3	*<Dataverlies (Recovery-Point Objective (RPO)) en hersteltijd (Recovery-Time Objective (RTO)) zijn doelstellingen die een belangrijke rol spelen bij disaster recovery.* *Hoeveel dataverlies (RPO) is acceptabel en binnen welke tijdsperiode (RTO) moet de dienstverlening weer hersteld zijn?* *Deze vraag heeft betrekking op het dataverlies (RPO).>* *Vraag B3 heeft betrekking op de hersteltijd (RTO).*
	Subtotalen B1-B7					
Wat is de meest serieuze impact als het proces onbeschikbaar is?						*<Neem de hoogste score, per kolom, over van bovenstaande ingevulde impact waarderingen.>*
Wat is overall de meest serieuze impact als het proces onbeschikbaar is?						*<Neem de hoogste score over van bovenstaande ingevulde impact typeringen.>*

3 =	zeer ernstige schade met zeer hoge herstelkosten: de dienstverlening aan de burger/bedrijven/ketenpartners komt in gevaar, raadsvragen, reactie wethouder vereist, berichten in de krant, professionaliteit van het concern, de gemeentelijke dienst ter discussie.
2 =	ernstige schade met hoge herstelkosten: krantenkoppen, vragen van belangrijke partners/klanten, budgettaire problemen.
1 =	acceptabele, binnen marges, herstelbare schade en herstelkosten: incident met direct betrokkenen is snel recht te zetten.
0 =	verwaarloosbare schade en herstelkosten of niet van toepassing.

KWALITEITSINSTITUUT NEDERLANDSE GEMEENTEN IN OPDRACHT VAN VERENIGING VAN NEDERLANDSE GEMEENTEN

I – Vragenlijst integriteit

Het onderwerp integriteit valt normaliter in twee delen uiteen: de integriteit van data communicatie en opslag enerzijds (dat wil zeggen niet gerelateerd aan het gemeentelijke proces zelf), en de integriteit van de informatie in de applicaties of fysiek (dat wil zeggen 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.

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?

Bedrijfsproces (business) impact schaalverdeling:

0. Verwaarloosbaar
1. Belangrijke schade
2. Ernstige schade
3. Bedreigt het voortbestaan (van leden) van het college van B&W

KWALITEITSINSTITUUT NEDERLANDSE GEMEENTEN IN OPDRACHT VAN VERENIGING VAN NEDERLANDSE GEMEENTEN

Bedrijfsproces consequentie *(in het ergste geval)*	Bedrijfsproces impact				Argumentatie *(verplicht invullen)*
Wanneer maximale schade?	**0**	**1**	**2**	**3**	
Managementbeslissingen Hoe schadelijk is het als op basis van deze informatie verkeerde managementbeslissingen worden genomen?					
Fraude Welke impact hebben frauduleuze handelingen?					
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?					
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

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.

Vragenlijst vertrouwelijkheid
Om te bepalen óf en hoe vertrouwelijk informatie is, is het van belang te weten wat de bedrijfsproces 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 licentiebeperkingen)
g. Bevat het informatiebedrijfsmiddel gegevens die gebruikt kunnen worden om fraude te plegen? (denk bijv. aan identiteitsfraude, creditcardnummers, wachtwoordbestanden).

Bedrijfsproces (business) impact schaalverdeling:

0. Verwaarloosbaar
1. Belangrijke schade
2. Ernstige schade
3. Bedreigt het voortbestaan (van leden) van het college van B&W

KWALITEITSINSTITUUT NEDERLANDSE GEMEENTEN IN OPDRACHT VAN VERENIGING VAN NEDERLANDSE GEMEENTEN

Bedrijfsproces consequentie *(in het ergste geval)*	Bedrijfsproces impact				Argumentatie *(verplicht invullen)*
Wanneer maximale schade?	**0**	**1**	**2**	**3**	
Fraude Welke impact hebben frauduleuze handelingen t.g.v. bekend worden van deze gegevens?					
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?[19]					
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?					
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)					

[19] 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.

KWALITEITSINSTITUUT NEDERLANDSE GEMEENTEN IN OPDRACHT VAN VERENIGING VAN NEDERLANDSE GEMEENTEN

Bijlage 3: Waarderingsschaal

De in deze bijlage opgenomen waarderingsschaal 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-gegevens	**Wettelijke en reglementaire verplichtingen**	**Financieel verlies**	**Beleid en werking van de gemeentelijke overheid**	**Verlies van goodwill**
Enige schade **Bedrijfsproces impact=1**	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 **Bedrijfsproces impact=2**	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 **Bedrijfsproces impact=3**	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
V00R 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

INFO@IBDGEMEENTEN.NL
WWW.IBDGEMEENTEN.NL