TASKFORCE
Bestuur & Informatieveiligheid Dienstverlening

Dataclassificatie

Een operationeel product op basis van de Baseline Informatiebeveiliging Rijksdienst (BIR)

Rijksoverheid VNG Vereniging van Nederlandse Gemeenten Interprovinciaal Overleg ip MANIFESTgroep UNIE VAN WATERSCHAPPEN

Colofon

Onderhavig operationeel product, behorende bij de Baseline Informatiebeveiliging Rijksdienst (BIR), is mogelijk gemaakt door de Taskforce Bestuur en Informatieveiligheid Dienstverlening (Taskforce BID). Het product is gebaseerd op het operationele product ‘Handreiking Dataclassificatie’ behorende bij de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG). Dit product is ontwikkeld door de Informatiebeveiligingsdienst voor gemeenten (IBD).

Leeswijzer

Dit document is een van de operationele producten op basis van de Baseline Informatiebeveiliging Rijksdienst (BIR).

Doel

Dit document beschrijft de beleidsuitgangspunten ten aanzien van informatiebeveiliging voor een invulling van het dataclassificatiebeleid door organisaties binnen de Rijksoverheid. Deze uitgangspunten over informatiebeveiliging zijn afkomstig uit de BIR en het beleid voldoet daarmee aan de BIR.

Doelgroep

Dit document is van belang voor systeemeigenaren en informatiemanagers.

Reikwijdte

Dit document heeft voornamelijk betrekking op maatregel 7.2 van de Baseline Informatiebeveiliging Rijksdienst (BIR). Het document gaat in op personele, organisatorische en technische informatiebeveiligingsaspecten die organisaties binnen de Rijksoverheid dienen te overwegen in relatie tot dataclassificatie.

Relatie met overige producten

- Baseline Informatiebeveiliging Rijksdienst (BIR). Tactisch Normenkader (TNK)
- Voorschrift Informatiebeveiliging Rijksdienst (VIR:2007)
- Voorschrift Informatiebeveiliging Rijksdienst - Bijzondere Informatie (VIRBI:2013)
- Informatiebeveiligingsbeleid
- GAP-analyse
- Quick scan BIR

Inhoudsopgave

1 Inleiding

Dit document bevat een good practice voor (data)classificatie (ook wel rubricering genoemd). Data betekent in dit verband alle gegevens en informatie, ongeacht het medium waarop deze opgeslagen wordt en ongeacht de presentatie daarvan. Classificatie van data maakt het mogelijk voor te schrijven welke maatregelen moeten worden genomen om die bepaalde data adequaat te beschermen. Tegelijkertijd geeft het antwoord op de vraag of de bepaalde data binnen of buiten de reikwijdte van de baseline valt.

De in deze handreiking genoemde niveaus en (bewaar)termijnen zijn een voorstel gebaseerd op verschillende brondocumenten, waaronder: wetgeving, het Voorschrift Informatiebeveiliging Rijksdienst en PvIB patronen.

De maatregel dataclassificatie komt voort uit de tactische variant van de Baseline Informatiebeveiliging Rijksdienst (BIR), hoofdstuk 7.2. Dit document biedt handvatten om een eigen classificatiesysteem te ontwikkelen of te verbeteren en deze te implementeren.

1.1 Belang van classificatie

De voorgestelde classificatiemethodiek geeft een snelle indicatie van het belang van de informatie(systemen) en is daarmee een basis voor een risicoanalyse. 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 gebruik van standaard hulpmiddelen voor risicoanalyse is vaak een tijdrovend en abstract traject. Na de classificatie kunnen de juiste maatregelen getroffen worden waardoor inbreuken op de veiligheid worden voorkomen met een beperkte inzet van middelen.

2 Classificatie van data

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.

Met de invoering van de Baseline Informatiebeveiliging Rijksdienst (BIR) is het basis beveiligingsniveau bepaald dat geldt voor de gehele bedrijfsvoering van een overheidsorganisatie. 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 is dan ‘vertrouwelijk’, het basisniveau van de BIR, dan zijn extra maatregelen nodig. Soms zijn deze maatregelen al genomen als application control (binnen de applicatie). In andere gevallen zijn deze extra maatregelen al uitgewerkt door een uitgevoerde risicoanalyse van een andere organisatie of er wordt binnen de organisatie een risicoafweging gemaakt door het uitvoeren van een risicoanalyse met als resultaat meer passende maatregelen.

2.1 Risicoanalyse

Een organisatie 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. 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 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 kunnen worden beheerst, of worden teruggebracht tot een aanvaardbaar niveau. Dit kan door 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 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 worden bepaald welke beveiligingsmaatregelen moeten worden getroffen om de risico’s terug te dringen. Vooral bij de vertaling van risico’s naar passende maatregelen is classificatie een belangrijk hulpmiddel om de ernst van een risico en de reikwijdte van een maatregel te kunnen bepalen. De hier voorgestelde classificatie kan worden beschouwd als een vereenvoudigde vorm van een risicoanalyse.

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

2.2 Beschermingsniveau van data

Het beschermingsniveau van data wordt uitgedrukt in classificatieniveaus ten aanzien van de beschikbaarheid, integriteit en vertrouwelijkheid van informatie. Onderstaande classificatie is een voorbeeld om een eigen classificatiesysteem te ontwikkelen of te verbeteren en deze te implementeren. Door onderstaande classificatie te hanteren is het eenvoudig aan te sluiten op de baseline (zie stap 5 in hoofdstuk 5).

Beschikbaarheid

Beschikbaarheid beschrijft hoeveel en wanneer data toegankelijk is en kan worden gebruikt. De onderscheiden niveaus van beschikbaarheid zijn:

- Niet nodig: De gegevens kunnen zonder gevolgen langere tijd niet beschikbaar zijn Schending van beschikbaarheid heeft geen gevolgschade.
- Belangrijk: De informatie of service kan incidenteel uitvallen, het bedrijfsproces staat incidentele uitval toe. De continuïteit zal op redelijke termijn moeten worden hervat. Schending van deze classificatie kan enige[1] (in)directe schade toebrengen
- Noodzakelijk: De informatie of service zou niet moeten uitvallen, het bedrijfsproces staat nauwelijks uitval toe. De continuïteit zal snel moeten worden hervat. Schending van deze classificatie kan serieuze[2] (in)directe schade toebrengen.
- Essentieel: De informatie of service behoort alleen in zeer uitzonderlijke situaties uit te vallen, 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[3] schade toebrengen.

Integriteit

Integriteit gaat over 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 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 heeft geen directe hinder van (integriteits)fouten. 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.

[123] Voor uitleg over ‘enige’, ‘serieuze’ en ‘zeer grote’ zie bijlage 3

- Absoluut: Het bedrijfsproces dat gebruik maakt van deze informatie staat geen (integriteits)fouten toe. Schending van integriteit kan (zeer) grote schade toebrengen

Vertrouwelijkheid

Vertrouwelijkheid beschrijft de bevoegdheden en de mogelijkheden tot muteren, kopiëren, toevoegen, vernietigen of kennisnemen van informatie voor een gedefinieerde groep van gerechtigden. 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 gebruikers[4]. De informatie wordt ter beschikking gesteld op basis van vertrouwen. Schending van deze classificatie kan serieuze (in)directe schade toebrengen.
- Geheim: Dit betreft gevoelige informatie die alleen toegankelijk mag zijn voor de direct geadresseerde. Schending van deze classificatie kan zeer grote schade toebrengen.

[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.

3 Principes voor classificatie

De volgende principes vormen de uitgangspunten voor (data)classificatie:

Alle gegevens

De classificatietabel heeft betrekking op alle in beheer zijnde gegevensverzamelingen, gegevensdragers, informatiesystemen, servers en netwerkcomponenten.

Informatie juist beschermen

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 in een informatiesysteem daarvoor maatregelen (applicatie controls) genomen zijn om delen van de systeeminformatie die hoger geclassificeerd is adequaat te beschermen op record- of schermniveau, dan kan een systeem als geheel lager worden ingeschaald binnen de tabel. Het systeem kan bijvoorbeeld daarmee alsnog binnen de baseline vallen.

Eigenaar blijft verantwoordelijk

De eigenaar van de gegevens en de proceseigenaar bepalen de vereiste beschermingsniveaus (classificaties). Indien sprake is van wettelijke eisen wordt dit expliciet aangegeven. De eigenaar van de gegevens bepaalt tevens wie toegang krijgt tot welke gegevens. In alle gevallen kan de eigenaar van de gegevens zich voor het classificeren laten ondersteunen door beveiligingsspecialisten, zoals de CISO.

Streven naar een zo laag mogelijk classificatieniveau

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.

BIR vormt het uitgangspunt

De BIR vormt de baseline. Als er additionele maatregelen noodzakelijk zijn dan worden deze *risicogebaseerd* geformuleerd en geïmplementeerd. Dit houdt in dat maatregelen worden afgestemd op de risico’s, waarbij rekening gehouden te worden dient met technische mogelijkheden en de kosten van de te nemen maatregelen

4 Beveiligingseisen per classificatieniveau

4.1 Beschikbaarheid

Beschikbaarheid is gedefinieerd als *'eigenschap 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.

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.

4.1.1 Beveiligingsnormen

De onderstaande tabel beschrijft de beveiligingseisen en maatregelen per classificatieniveau ten aanzien van beschikbaarheid. De in de onderstaande tabel genoemde waarden dienen als voorbeeld. De waarden moeten door de organisatie zelf worden bepaald.

De normen voor de kantoor Automatisering (KA), Intranet en de toegevoegde diensten kunnen als volgt worden ingevuld: *(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: 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 minuten)	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.)

MTTR (voor storingen langer dan 3 minuten)	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 minuten)	4 uur	(max.)
Aantal storingen:		
3 Minuten of korter	1 per maand	(max.)
Langer dan 3 minuten	1 per halfjaar	(max.)

4.2 Integriteit

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

Het onderwerp integriteit valt normaliter in twee delen uiteen: (1) de integriteit van data communicatie en opslag. Dit is niet gerelateerd aan het organisatieproces zelf; en (2) de integriteit van de informatie in de applicaties of fysiek. Dit is gerelateerd aan het organisatieproces. Integriteit in de tweede vorm, gekoppeld aan de applicatie, is altijd situatieafhankelijk 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 kunnen worden gemaakt.

4.2.1 Beveiligingsnormen integriteit

De onderstaande tabel beschrijft de beveiligingseisen en maatregelen per classificatieniveau ten aanzien van integriteit. Integriteit is onderverdeeld in eisen voor authenticatie, autorisatie, monitoring en beveiliging. De bewaartermijnen zijn indicatief. Voor gegevens waarin (herleidbare) persoonsgegevens voorkomen, moet betreffende een bewaartermijn van meer dan zes maanden formeel melding worden gedaan bij de privacyfunctionaris 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.[67] Na uitvoering van een service blijven gewijzigde gegevens consistent.

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

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 jaar[8] 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 in de tabel verwijzen naar het vereiste beveiligingsmechanisme:

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

[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 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 Rijksdienst.

4.3 Vertrouwelijkheid

Vertrouwelijkheid waarborgt dat alleen geautoriseerden toegang krijgen tot als vertrouwelijk aangemerkte informatie. Vertrouwelijkheid is eveneens een kwaliteitskenmerk van gegevens en gegevensverwerkingen, maar anders dan integriteit is vertrouwelijkheid een gradueel begrip: voor verschillende belanghebbenden of belangstellenden kan informatie meer of minder vertrouwelijk zijn. Wie toegang tot de informatie krijgt wordt bepaald door de eigenaar.

Vertrouwelijke gegevens zijn bijvoorbeeld:

- Persoonsgegevens
- Organisatie- en bedrijfsgeheimen
- Concurrentiegevoelige gegevens, zoals voorbereidingen voor bestemmingsplannen
- Medische gegevens

4.3.1 Beveiligingsmaatregelen

De 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 <organisatie> 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 gegevenseigenaar 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 <organisatie> 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	Authenticatie 'hoog' vereist. Sessie-timeout na 15 min inactiviteit. Voor klant absolute	Autorisatie vereist (specifieke rol).	Vastleggen correcte en foutieve authenticatie en tijdstip. Monitoring-gegevens bewaren	Outputvalidatie. Versleuteling tijdens transport en op tussenstations via berichtbeveiliging. Versleutelde opslag van

[9] 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'.
[10] Ontwikkel-, Test- en Acceptatie- omgevingen.

	sessie-timeout na 120 min. Identiteit blokkeren na 3 achtereenvolgende foutieve authenticatiepogingen. Authenticatie 'hoog' nodig voor deblokkeren. Geen SSO toegestaan.		voor periode van 7 jaar.	gegevens. Transport van gegevens minimaliseren. Alleen transport en opslag binnen vaste netwerk van <organisatie>. 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 authenticatieniveaus verwijzen naar het vereiste beveiligingsmechanisme (zie voorgaande paragraaf). Bedrijfsvertrouwelijk verwijst naar de 'organisatie', waarmee wordt bedoeld: de gehele organisatie, organisatieonderdeel of een dienst.

5 Bepalen van classificatieniveaus

In de voorgaande hoofdstukken is de context beschreven bij het toekennen van classificatieniveaus: de beleidsuitgangspunten, architectuurprincipes en beveiligingseisen. In dit hoofdstuk zijn de stappen beschreven waarmee data kan worden geclassificeerd.

Stap 1: Wettelijke eisen

De eerste stap bij dataclassificatie is bepalen 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 Rijksdienst (BIR).

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 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 of niet is toegestaan, 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 ten aanzien van 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? 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. 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 ten behoeve van 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 bedrijfsvoeringsprocessen voor de organisatie en hoe deze processen worden ondersteund door de ICT-voorzieningen.

De analyse kan worden 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, wordt sterk aanbevolen om de ingevulde vragenlijsten te archiveren.

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

Classificeren is geen exacte wetenschap. Het bepalen van het classificatieniveau volgt uit een risicobeoordeling waarin de 'waarde' van informatie wordt bepaald. Aangezien de 'waarde' lang niet altijd meetbaar is, is toekenning van een classificatieniveau soms arbitrair. In die gevallen kan een afweging worden gemaakt 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.

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.

Het classificeren van data kan het beste door stakeholders in een workshopverband worden uitgevoerd. 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.

Mocht de uitkomst van de analyse uitkomen onder of op de baselineniveaus, dan hoeven geen extra maatregelen genomen te worden. Het beveiligingsniveau van de baseline is zo gekozen dat dit voor de meeste processen en ondersteunende ICT-voorzieningen bij overheidsorganisaties voldoende is. Hiermee wordt voorkomen dat er voor ieder systeem een uitgebreide risicoanalyse uitgevoerd moet worden. Als één van de ‘BIV-waarden’ een hogere score heeft dan hieronder genoemd, dan moeten er extra maatregelen genomen worden. Deze maatregelen worden separaat beschikbaar gesteld als aanvullende maatregelen al naar gelang de BIV-score.

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

- Beschikbaarheid: Belangrijk
- Integriteit: Hoog
- Vertrouwelijkheid: Vertrouwelijk

Bijlage 1: Classificatie leidraad

Het classificatieproces bij <organisatie> 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 organisatie.

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 <organisatie> geeft een inschaling op de volgende niveaus:

A. Beschikbaarheid :
B. Integriteit :
C. Vertrouwelijkheid :

Conclusie: Het proces <procesnaam> valt binnen/buiten de Baseline Informatiebeveiliging Rijksdienst (BIR) 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 restrisico 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 organisatie

Business consequentie	**Business impact**				
Wanneer maximale schade?	**uur**	**dag**	**week**	**2-3 weken**	**maand**
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 organisatie

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 licentiebeperkingen)
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 organisatie

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.