

## Informatieveiligheid volwassenheidsniveau 2

|                                |                                          |                                                                                                                                                                                                                                                          |                                                                                                                                                                                                                                                                                                       |
|--------------------------------|------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Informatiebeveiliging          | Scope bepalen:                           | Niveau 2 kenmerk project                                                                                                                                                                                                                                 | Volwassenheid 2 (herhaalbaar). Je ziet:<br>IB is een project                                                                                                                                                                                                                                          |
|                                | Monitoring                               | Planning en control<br>DT Strategisch<br>MGT Tactisch<br>Afd Operationeel                                                                                                                                                                                | Zaken worden opgestart maar meestal verder niet gevolgd (plan, do, geen check, geen act)<br>Vooruitkijken en beleidskeuzes maken is informeel en niet geïntegreerd<br>Vertaling van beleid vindt plaats op basis van persoonlijk inzicht<br>Toepassing van regels vindt plaats op persoonlijk inzicht |
| Onderbouwing (aantoonbaarheid) | CISO is projectleider                    | De CISO probeert management aandacht te krijgen voor het onderwerp en mensen te betrekken                                                                                                                                                                |                                                                                                                                                                                                                                                                                                       |
|                                | CISO maakt Informatie beveiligingsbeleid | Risicoanalyses informeel en soms gedeeld met de werkvloer. Procedures zijn op hoofdlijnen aanwezig                                                                                                                                                       |                                                                                                                                                                                                                                                                                                       |
|                                | Aanjagers helpen de CISO                 | Kwaliteit is niet expliciet gedefinieerd, maar de gewenste kwaliteit van de resultaten is voldoende bekend bij de medewerkers en wordt grotendeels consistent geleverd. Er is geen inzicht in kwalitatieve en kwantitatieve prestaties van de processen. |                                                                                                                                                                                                                                                                                                       |
|                                | Incident management                      | Incidenten worden informeel afgehandeld en worden persoonsafhankelijk opgelost. Aanpassingen in processen worden niet volledig gecommuniceerd en dus niet altijd toegepast in de praktijk.                                                               |                                                                                                                                                                                                                                                                                                       |
| Mensen                         | CISO en ICT betrokken                    | Elke medewerker verdiept zich naar eigen inzicht en behoefte in Informatiebeveiliging                                                                                                                                                                    |                                                                                                                                                                                                                                                                                                       |
|                                | Goed huisvaderschap                      | TBV zijn bekend bij medewerkers maar niet expliciet gedefinieerd.                                                                                                                                                                                        |                                                                                                                                                                                                                                                                                                       |
|                                | Eerste ervaringen                        | Er is enige bewustwording over wat gewenst en ongewenst gedrag is in de omgang met bedrijfsinformatie                                                                                                                                                    |                                                                                                                                                                                                                                                                                                       |
| Inrichting en structuur        | BIO controls (BBN2) aanwezig (opzet)     | Meeste verplichte overheidsmaatregelen zijn toegepast en classificatie van informatie is deels op orde. Er is nog ongeclassificeerde informatie in gebruik.                                                                                              |                                                                                                                                                                                                                                                                                                       |

## Informatieveiligheid volwassenheidsniveau 3

|                                   |                                                                                  |                                                                                                                                                                                 |                                                                                                                      |
|-----------------------------------|----------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------|
| Informatiebeveiliging             |                                                                                  | Niveau 3 kenmerk                                                                                                                                                                | Volwassenheid 3 (gedefinieerd). Je ziet:                                                                             |
| Scope bepalen:                    |                                                                                  | apart proces                                                                                                                                                                    | IB is een proces                                                                                                     |
| Monitoring                        | Planning en control                                                              | Zaken worden gepland opgestart en soms gevolgd (plan, do, beperkt check, geen act)                                                                                              |                                                                                                                      |
|                                   | DT Strategisch                                                                   | Een formeel vastgestelde visie en beleid voor informatiebeveiliging                                                                                                             |                                                                                                                      |
|                                   | MGT Tactisch                                                                     | Het beleid is geoperationaliseerd naar methodes voor de afgewogen toepassing van maatregelen in systemen en projecten (BIVclassificaties van data of systemen of architectuur). |                                                                                                                      |
|                                   | Afd Operationeel                                                                 | Toepassing van regels vindt plaats op gemeenschappelijk inzicht (bijvoorbeeld per proces, per afdeling)                                                                         |                                                                                                                      |
|                                   |                                                                                  |                                                                                                                                                                                 |                                                                                                                      |
| Onderbouwing<br>(aantoonbaarheid) |                                                                                  | IB is in relevante procedures voldoende gedefinieerd. TBV zijn gecommuniceerd naar medewerkers.                                                                                 |                                                                                                                      |
|                                   | CISO en PE maken IB beleid, IB plan en IB producten en besturen het proces samen | Informeel risico analyses, afhankelijk van eigen inzicht                                                                                                                        |                                                                                                                      |
|                                   |                                                                                  | Kwaliteit van resultaten op hoofdlijnen gedefinieerd. Geen kwaliteitscontrole intern en extern (beperkt IB contractmanagement)                                                  |                                                                                                                      |
|                                   |                                                                                  | Incidenten worden op de werkvloer geanalyseerd en behandeld, en leiden tot aanpassingen in de processen.                                                                        |                                                                                                                      |
|                                   |                                                                                  |                                                                                                                                                                                 |                                                                                                                      |
| Mensen                            | PE en medewerkers leren en bekwamen zich stapsgewijs                             | Jaarlijkse opleidingen en awareness.                                                                                                                                            |                                                                                                                      |
|                                   |                                                                                  | Beperkt voorbeeldgedrag van mgt. Mensen weten wat ze moeten bijdragen maar dat lukt nog niet altijd. Trainingen worden sctructueel gevolgd.                                     |                                                                                                                      |
|                                   |                                                                                  | Er is groeiende bewustzijn over wat gewenst en ongewenst gedrag is in het veilig werken met bedrijfsinformatie                                                                  |                                                                                                                      |
|                                   |                                                                                  |                                                                                                                                                                                 |                                                                                                                      |
| Inrichting en structuur           |                                                                                  | BIO-controls (BBN2) zijn in gebruik (bestaan)                                                                                                                                   | Verplichte overheidsmaatregelenworden toegepast en classificatie van alle informatie die in gebruik is is vastgelegd |

## Informatieveiligheid volwassenheidsniveau 4

|                                                |                                                     |                                                                                                                                                                                                                                     |
|------------------------------------------------|-----------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Informatiebeveiliging</b><br>Scope bepalen: | Niveau 4 kenmerk<br>geïntegreerd                    | Volwassenheid 4 (beheerst). Je ziet:<br>IB is onderdeel van bedrijfsprocessen                                                                                                                                                       |
| <b>Monitoring</b>                              | Planning en control                                 | PDCA gestructureerd aanwezig, bijvoorbeeld in jaarplannen                                                                                                                                                                           |
|                                                | DT Strategisch                                      | Nieuwe ontwikkelingen op het gebied van wet- en regelgeving en bedreigingen worden gesignaleerd en verwerkt in de strategische planning en risk appetite van de organisatie                                                         |
|                                                | MGT Tactisch                                        | Het informatiebeveiligingsbeleid is geoperationaliseerd naar methodes voor afgewogen leuzes (risico management, kosten/baten) en daarna gerealiseerd in maatregelen                                                                 |
|                                                | Afd Operationeel                                    | Het beleid voor informatiebeveiliging en de BIV classificaties wordt periodiek geëvalueerd op de uitvoering in de praktijk. De gerealiseerde maatregelen worden geëvalueerd en bijgesteld                                           |
| <b>Onderbouwing<br/>(aantoonbaarheid)</b>      | PE zelf aan zet                                     | Active intervisie op best practises, aantoonbare sturing op de BIO en Informatiebeveiligingbeleid, zelf evaluatie en risico management. ISMS bijhouden                                                                              |
|                                                | CISO houdt toezicht op beleid                       | Interne en externe audits en metingen,. Risico impact assessments beoordelen, ISMS volgen                                                                                                                                           |
|                                                | Vastgestelde processen en documentatie              | Processen zijn vastgesteld en worden geevalueerd. IB Risicoanalyse en regelmatige review. Kwaliteit van resultaten is gedefinieerd (KPI's). Contractmanagement met IB als paragraaf is ingebed in het beheer van de externe dienst. |
|                                                | Kwaliteitsverbetering                               | Proactieve monitoring op het detecteren van incidenten vindt plaats. Centrale analyse en incidenten leiden tot verbetering en communicatie                                                                                          |
| <b>Mensen</b>                                  | Onbewust en aantoonbaar doen aan IB                 | Leidinggevend en geven voorbeeldgedrag en verbinden consequenties aan ongewenst gedrag<br>Mensen committeren zich (expliciet) aan het leveren van een bijdrage aan goede informatiebeveiliging                                      |
|                                                | Continuïteit in leren                               | Mensen delen onderling kennis, 'best practices' en ervaringen over de omgang met informatiebeveiliging. Meerjarig opleidingsplan                                                                                                    |
| <b>Inrichting en structuur</b>                 | BIO-controls (BBN2 en BBN2+) zijn in orde (werking) | Verplichte overheidsmaatregelen en risico assessment indien dat nodig is wegens het belang van de informatie voor de organisatie Vastgestelde regels worden in de praktijk door iedereen toegepast.                                 |

## Privacy volwassenheidsniveau 2

| PRIVACY                            | Niveau 2 kenmerk                            | Volwassenheid niveau 2 (proces is herhaalbaar). Je ziet:                                                                                                                                                                                                 |
|------------------------------------|---------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Scope bepalen:                     | project                                     | Privacy is een project                                                                                                                                                                                                                                   |
|                                    |                                             |                                                                                                                                                                                                                                                          |
| Monitoring                         | Planning en control                         | Zaken worden opgestart maar meestal verder niet gevolgd (plan, do, geen check, geen act)                                                                                                                                                                 |
|                                    | DT Strategisch                              | Vooruitkijken en beleidskeuzes maken is informeel en niet geïntegreerd                                                                                                                                                                                   |
|                                    | MGT Tactisch                                | Vertaling van beleid naar uitvoering vindt plaats op basis van persoonlijk inzicht                                                                                                                                                                       |
|                                    | Afd Operationeel                            | Toepassing van regels vindt plaats obv persoonlijk inzicht                                                                                                                                                                                               |
|                                    |                                             |                                                                                                                                                                                                                                                          |
| Onderbouwing<br>(aantoonbaar-heid) | FG is vooral projectleider                  | De FG probeert management aandacht te krijgen voor het onderwerp en mensen te betrekken                                                                                                                                                                  |
|                                    | FG maakt het privacybeleid                  | Risicoanalyses informeel, in het hoofd en soms gedeeld met de werkvloer. Procedures zijn op hoofdlijnen aanwezig                                                                                                                                         |
|                                    | Aanjagers helpen de FG                      | Kwaliteit is niet expliciet gedefinieerd, maar de gewenste kwaliteit van de resultaten is voldoende bekend bij de medewerkers en wordt grotendeels consistent geleverd. Er is geen inzicht in kwalitatieve en kwantitatieve prestaties van de processen. |
|                                    | Datalekken                                  | Datalekken worden informeel afgehandeld en worden persoonsafhankelijk opgelost. Aanpassingen in processen worden niet volledig gecommuniceerd en worden dus niet altijd toegepast in de praktijk. Datalek blijft soms onzichtbaar.                       |
|                                    |                                             |                                                                                                                                                                                                                                                          |
| Mensen                             | FG en JZ betrokken                          | Elke medewerker (of team) verdiept zich naar eigen inzicht en behoefte in privacy. "Ik heb niets te verbergen", hoor je vaak.                                                                                                                            |
|                                    | Goed huisvaderschap                         | TBV zijn bekend bij medewerkers maar niet expliciet gedefinieerd.                                                                                                                                                                                        |
|                                    | Eerste ervaringen met het onderwerp privacy | Er is enige bewustwording over wat gewenst en ongewenst gedrag is in de verwerking van persoonsgegevens                                                                                                                                                  |
|                                    |                                             |                                                                                                                                                                                                                                                          |
| Inrichting en structuur            | AVG 10-basisvereisten zijn aanwezig (opzet) | De 10 basisvereisten worden af en toe gebruikt, meestal alleen als het uitkomt.                                                                                                                                                                          |

### Privacy volwassenheidsniveau 3

| PRIVACY                            | Niveau 3 kenmerk                                                      | Volwassenheid 3 (proces is gedefinieerd). Je ziet:                                                                                                                              |
|------------------------------------|-----------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Scope bepalen:                     | apart proces                                                          | Privacy is een apart proces                                                                                                                                                     |
|                                    |                                                                       |                                                                                                                                                                                 |
| Monitoring                         | Planning en control                                                   | Zaken worden meestal gepland opgestart en soms gevolgd (Plan, do, beperkte check en soms act)                                                                                   |
|                                    | DT Strategisch                                                        | Een formeel vastgestelde visie en beleid voor privacy en informatiebeveiliging                                                                                                  |
|                                    | MGT Tactisch                                                          | Het beleid is geoperationaliseerd naar methodes voor de afgewogen toepassing van maatregelen in systemen en projecten (BIVclassificaties van data of systemen of architectuur). |
|                                    | Afd Operationeel                                                      | Toepassing van regels vindt plaats obv gemeenschappelijk inzicht (bijv per proces, per afdeling)                                                                                |
|                                    |                                                                       |                                                                                                                                                                                 |
| Onderbouwing<br>(aantoonbaar-heid) | FG en PE maken beleid, plan en producten en besturen het proces samen | Privacy is in relevante procedures voldoende gedefinieerd. TBV zijn gecommuniceerd naar medewerkers.                                                                            |
|                                    |                                                                       | Privacy advies (juridisch, PIA) wordt indien gevraagd altijd opgevolgd. Het wordt niet altijd gevraagd.                                                                         |
|                                    |                                                                       | Kwaliteit van resultaten op hoofdlijnen gedefinieerd. Geen kwaliteitscontrole                                                                                                   |
|                                    |                                                                       | Incidenten en datalekken worden op de werkvloer geanalyseerd , behandeld, en geregistreerd en leiden al in veel gevallen tot aanpassingen in de processen.                      |
|                                    |                                                                       |                                                                                                                                                                                 |
| Mensen                             | PE en medewerkers leren en bekwamen zich stapsgewijs                  | Jaarlijkse opleidingen en awareness. Het onderwerp leeft al wel bij de meeste medewerkers die met (gevoelige/veel) persoonsgegevens werken.                                     |
|                                    |                                                                       | Beperkt voorbeeldgedrag van mgt. Mensen weten wat ze moeten bijdragen maar dat lukt nog niet altijd. Trainingen worden structureel gevolgd.                                     |
|                                    |                                                                       | Er is groeiende bewustwording over wat gewenst en ongewenst gedrag is in de verwerking van persoonsgegevens                                                                     |
|                                    |                                                                       |                                                                                                                                                                                 |
| Inrichting en structuur            | AVG 10-basisvereisten zijn in gebruik (bestaan)                       | De 10 basisvereisten worden in belangrijke gevallen gebruikt, administraties zijn inhoudelijk nog niet op orde (80-20 regel)                                                    |

## Privacy volwassenheidsniveau 4

| PRIVACY                            | Niveau 4 kenmerk                             | Volwassenheid 4 (beheerst). Je ziet:                                                                                                                                                                                                           |
|------------------------------------|----------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Scope bepalen:                     | geïntegreerd                                 | Privacy is onderdeel van verwerken van persoonsgegevens (in ieder relevant proces)                                                                                                                                                             |
|                                    |                                              |                                                                                                                                                                                                                                                |
| Monitoring                         | Planning en control                          | PDCA gestructureerd aanwezig, bijvoorbeeld in jaarplannen                                                                                                                                                                                      |
|                                    | DT Strategisch                               | Nieuwe ontwikkelingen op het gebied van privacywet- en regelgeving worden gesignaleerd en verwerkt in de strategische planning van de organisatie                                                                                              |
|                                    | MGT Tactisch                                 | Het beleid voor privacy en informatiebeveiliging is geoperationaliseerd naar methodes voor afgewogen leuzes (risico management en kosten/baten voor personen (betrokkenen) en daarna gerealiseerd in maatregelen                               |
|                                    | Afd Operationeel                             | Het beleid voor privacy en de classificatie van persoonsgegevens wordt periodiek geëvalueerd op de uitvoering in de praktijk. De gerealiseerde maatregelen worden geëvalueerd en bijgesteld                                                    |
|                                    |                                              |                                                                                                                                                                                                                                                |
| Onderbouwing<br>(aantoonbaar-heid) | PE is zelf aan zet                           | Active intervisie op best practises, aantoonbare sturing op het AVG, zelf evaluatie, zoekt de FG zelf op voor advies                                                                                                                           |
|                                    | FG houdt toezicht op beleid                  | Interne en externe audits, DPIA beoordelen, contact met de Autoriteit Persoonsgegevens                                                                                                                                                         |
|                                    | Vastgestelde processen en documentatie       | Processen zijn vastgesteld en worden geëvalueerd. Risicoanalyse en regelmatige review. Kwaliteit van resultaten is gedefinieerd (KPI's). PE's voeren zelf de administratie (register van verwerkingen) en beheren hun verwerkersovereenkomsten |
|                                    | Kwaliteitsverbetering                        | Proactieve monitoring op het detecteren van incidenten vindt plaats in het verwerkende proces. Centrale analyse van incidenten en problemen leiden tot verbetering en communicatie                                                             |
|                                    |                                              |                                                                                                                                                                                                                                                |
| Mensen                             | Onbewust en aantoonbaar doen aan privacy     | Leidinggevend en geven voorbeeldgedrag en verbinden consequenties aan ongewenst gedrag                                                                                                                                                         |
|                                    |                                              | Medewerkers en leiding committeren zich (expliciet) aan het leveren van een bijdrage aan goede informatiebeveiliging en het borgen van privacy.                                                                                                |
|                                    | Continuïteit in leren                        | Mensen delen onderling actief kennis, 'best practices' en ervaringen over de omgang met privacy en informatiebeveiliging. Meerjarig opleidingsplan                                                                                             |
|                                    |                                              |                                                                                                                                                                                                                                                |
| Inrichting en structuur            | AVG 10-basisvereisten zijn in orde (werking) | De 10 basisvereisten worden altijd gebruikt, administraties zijn inhoudelijk meestal op orde (90-10 regel)                                                                                                                                     |