

Business Impact Analyse, Checklist vaststellen Classificatie-niveau en Privacy Impact.

Deze wordt toegevoegd aan PAD (of PID)

Betrouwbaarheids- en Privacyaspecten (BIVP-Classificatie)

Onze bedrijfsprocessen worden ondersteund door-, of zijn in grote mate afhankelijk van Informatiesystemen. Daarom is het noodzakelijk om, vanuit deze processen, de (business-)betrouwbaarheidseisen in kaart te brengen die we stellen aan de informatieverwerking zodat we niet verrast worden door incidenten en calamiteiten waardoor we operationele, financiële- en/of reputatieschade kunnen voorkomen of beperken. Met behulp van deze checklist brengen we de eisen in kaart.

ProRail wil voldoen aan de AVG. **Indien er dus persoonsgegevens verwerkt worden, worden de indicatoren “Vertrouwelijkheid” en “Integriteit” minimaal op “Middel” (2) gezet.** Afhankelijk van het Privacy Risico dient er een PIA (Privacy Impact Assessment) uitgevoerd te worden, t.b.v. het vaststellen van benodigde maatregelen.

Beschikbaarheid

- Beschrijf aan welke beschikbaarheidseisen het systeem/onderdeel moet voldoen.

Zie de tabellen in par. 4.3 van IBB 3.1

Hier zijn ook de verbanden tussen servicelevels en beschikbaarheid vastgelegd.

B = H / 3 (Goud)	Hoge Beschikbaarheid: De dienstverlening mag niet worden verstoord. Trein staat stil als de dienst uitvalt, er is bovenmatige externe overlast of er zijn extreme veiligheidsrisico's.
B = M / 2 (Zilver)	Medium beschikbaarheid: Applicatie moet ook beschikbaar zijn buiten kantooruren. Uitval veroorzaakt Extern overlast of overlast in keten.
B = L / 1 (Bronz +)	Lage Beschikbaarheid: Dienstverlening is slechts in geringe mate tijdsafhankelijk. Dienstverlening is binnen acht uur te herstellen.
B = B / 0 (Bronz)	Basis Beschikbaarheid: (Tijdelijk niveau) Reparatie bij uitval mogelijk met workaround, op "Best Effort" <i>Alleen voor reeds bestaande applicaties. Nieuw is Bronz+ de basis</i>

A	Hulpvragen of Servicematrix	B	L	M	H
	Meetpunten aan de hand van de service matrix:				
	Beschikbaarheid	Basaal (0)	Laag (1)	Midden (2)	Hoog (3)
	Tijdspan	Werkd 8-18u	Werkd 8-18u	7x24	7x24
	Totale beschikbaar.	<95%	<95%	95-99,5%	>99,5%
	Service Window	In kantooortijd	Ma-Do buiten kantooortijd	werk dagen 18u. t/m 7u. + weekend	Zondag van 01.00 tot 06.00 uur
	Functieherstel	80%<8u / 90%< 16u 99%<32u	80%<2u / 90%<8u / 99%<16u	80%<45m / 90%<2u / 99%<8u	
	Prioriteit 1				
B	Of: Meetpunten volgens BIZ:				
	1. Basis = B				
C	2. Verbeterd = L				
	3. Hoog = M				
	4. Continue = H				
	Of: Classificatiemethode op Servicelevel				
	Applicatie onderdeel van 7*24 bedrijfsvoering.				
	Gebruik buiten Kantooruren (7*24)				
	Bij OH Kantooruren overlast in keten > x gebr?				
	Workaround / uitstel tijdens OH niet goed mogelijk				
Keuze- matrix Service – level ICT-s	Ja				
	Nee				
	Bij Uitval Trein staat stil?				
	Ja				
	Nee				
	Bij uitval direct extern overlast?				
	Ja				
	Nee				
Keuze- matrix Service – level ICT-s	Bovenmatige Risico's 24Safety				
	Ja				
	Nee				
	GOUD				
	B(IV) = H(oog)				
	ZILVER				
	B(IV) = M(iddel)				
	B(IV) = L(aag)				
Keuze- matrix Service – level ICT-s	B(IV) = B(asaal)				
	BRONS PLU				
	BRONS				
	Deze altijd gebruiken In combinatie met de risicomatrix van ProRail !				
	B(IV) = B(asaal)				

Geef de motivatie hoe je tot de keuze gekomen bent. Dit is vooral belangrijk voor toekomstig gebruik

Totaal, cumulatief. Vul hier de hoogste waarde in voor **Beschikbaarheid** ➔

B* = M

Integriteit

I = H / 3	Hoge Integriteit: Informatie moet Gegarandeerd / <u>Bewezen</u> Correct zijn. Informatie waarbij het noodzakelijk is dat de correctheid niet betwist kan worden, zoals onomkeerbare financiële transacties met substantiële schade, productie- of persoonsgegevens. Grote schade voor ProRail indien deze gegevens niet correct zijn.
I = M / 2	Medium Integriteit: Informatie is Blijvend / <u>Geverifieerd</u> Correct. Sommige toleranties zijn toelaatbaar. Het is noodzakelijk dat de correctheid onbetwistbaar aangetoond kan worden. Indien de informatie niet correct is kan ProRail substantiële schade lijden.
I = L / 1	Lage Integriteit: Informatie is <u>aangenomen</u> Correct. Blijvende juistheid van informatie (vanaf de bron tot het laatste gebruik) is gewenst, maar niet vereist. Indien informatie niet correct is leidt dit tot weinig of geen schade. Voorbeelden: Interne telefoongidsen, agenda's enz.
I = B / 0	- Integriteit waarde B is niet in gebruik bij ProRail -

Hulpvragen + opmerkingen		L	M	H
A	Welk niveau van Integriteit is nodig om (factoren):			
	Juistheid: Is het belangrijk dat de juiste gegevens verstrekt worden. (b.v. het aantal wissels)			
	Correctheid: Is het belangrijk dat de gegevens te allen tijde correct zijn. (dat b.v. het aantal wissels in een rapportage juist is)			
	Volledigheid: Is het belangrijk dat de gegevens volledig zijn. (doet het exacte aantal er toe)			
	Tijdigheid: Is het belangrijk dat de gegevens altijd op tijd beschikbaar zijn, of mogen de gegevens eventueel iets ouder zijn.			
	Controleerbaarheid: Is het belangrijk om te weten welke gegevens wanneer aan wie verstrekt zijn.			
B	Of: beslisboom Integriteit: <pre> graph TD D1{ProRail leidt Onacceptabele schade bij inbreuk op de integriteit of ProRail voldoet niet meer aan wettelijke eisen bij een inbreuk op integriteit.} D2{ProRail leidt werkelijke schade, maar deze schade is te overzien.} D3{Verkeerde informatie is vervelend, maar niet kritisch. Er wordt geen meetbare schade geleden..} D1 -- Ja --> I1[I = Hoog] D1 -- Nee --> D2 D2 -- Ja --> I2[I = Middel] D2 -- Nee --> D3 D3 -- Ja --> I3[I = Laag] I1 --- B1[Bewezen Correct] I2 --- B2[Geverifieerd Correct] I3 --- B3[Aangenomen Correct] </pre>			
	Deze altijd gebruiken in combinatie met de risicomatrix van ProRail ! Bij verwerking van persoonsgegevens is de Integriteit minimaal M			
Geef de motivatie hoe je tot de keuze gekomen bent. Dit is vooral belangrijk voor toekomstig gebruik 				
Totaal, cumulatief. Vul hier de hoogste waarde in voor Integriteit →				
				I* = M

Vertrouwelijkheid

V = H / 3	Hoge Vertrouwelijkheid (Geheim) – ProRail kan grote schade leiden indien informatie toegankelijk is voor ongeautoriseerde personen. Informatie mag uitsluitend toegankelijk zijn voor een zeer selecte groep van personen. Bijvoorbeeld: ➢ Strategische plannen, informatie over toekomstige investeringen, samenwerkingsverbanden. ➢ Persoonlijke (medische) informatie zoals omschreven in risicoklasse III in het kader van de WBP ➢ Specificatie van de beveiligingscomponenten, inhoudelijke informatie over zeer ernstige beveiligingsincidenten, ed
V = M / 2	Medium vertrouwelijkheid (Vertrouwelijk) – ProRail kan substantiële schade lijden indien informatie toegankelijk is voor ongeautoriseerde personen. Informatie is alleen toegankelijk voor personen die hier vanuit hun functie toegang toe moeten hebben (need to know). Hieronder vallen ook persoonsgegevens.
V = L / 1	Lage vertrouwelijkheid (Intern) – Informatie is bedoeld voor Intern gebruik. Openbaar worden van gegevens leidt tot weinig of geen schade. Bijvoorbeeld: Algemene informatie over klanten, breed toegankelijke informatie op Intranet, beleidsdocumenten enz.
V = B / 0	Geen vertrouwelijkheid (Publiek of openbaar): Informatie is openbaar, bestemd voor iedereen, vrij toegankelijk. Bijvoorbeeld: Publieke informatie op een website, op folders, in brochures.

Hulpvragen + opmerkingen		B	L	M	H
A	Welk niveau van Vertrouwelijkheid is nodig om: • te voorkomen dat gegevens in de handen van vreemden komen? • verlies van orders en/of opdrachten te voorkomen? • frauduleuze aanwending van goederen en/of fondsen te voorkomen? • te verhinderen dat wettelijke of contractuele verplichtingen verbroken kunnen worden? • beschadiging van het moreel van het personeel en reizigers te kunnen voorkomen? • de bedrijfsvoering niet te verstoren?				
B	Of Beslisfactoren: • Vertrouwelijkheid van de gegevens die uitgewisseld worden met derden • Vertrouwelijkheid van gegevens die in interne systemen worden • Vertrouwelijkheid van gegevens die op systemen worden opgeslagen in DMZs • Worden er wachtwoorden gebruikt, anders dan one-time passwords? Één van deze? factoren, dan is de vertrouwelijk per definitie middel of hoog!				
C	Of: beslisboom Vertrouwelijkheid: <pre> graph TD D1{Bedrijfscontinuïteit ProRail komt in gevaar bij uitlekken van deze informatie of mensen leiden onherstelbare schade.} -- Ja --> V1[V = Hoog Geheim] D1 -- Nee --> D2{ProRail leidt grote schade bij uitlekken informatie (> € 500k of voorpagina nieuws).} D2 -- Ja --> V2[V = Middel Vertrouwelijk] D2 -- Nee --> D3{ProRail leidt werkelijke schade, maar deze schade is te overzien.} D3 -- Ja --> V3[V = Laag Intern / Intern+partners] D3 -- Nee --> B1[Publieke informatie, of uitlekken informatie geeft geen wezenlijke schade..] B1 --> V4[V = Basaal Publiek] </pre>				
Bij verwerking van persoonsgegevens is de Vertrouwelijkheid minimaal M					
Geef de motivatie hoe je tot de keuze gekomen bent. Dit is vooral belangrijk voor toekomstig gebruik					
Totaal, cumulatief. Vul hier de hoogste waarde in voor Vertrouwelijkheid →					
					V* = M

d

Privacy

P = H / 3	Hoog privacy risico – Betrokkenen kunnen grote schade oplopen indien er sprake is van een datalek. Bijvoorbeeld: ➢ Verwerking van bijzondere persoonsgegevens of strafrechtelijke gegevens ➢ Profiling / evaluatie op basis van persoonsgegevens met rechtsgevolgen ➢ Grootschalig en systematische volgen van mensen in publiek toegankelijk gebied (b.v. cameratoezicht)
P = M / 2	Medium privacy gevoeligheid – het betreft een verwerking van persoonsgegevens, niet zijnde bijzondere of vergelijkbare gegevens. Bijvoorbeeld het vastleggen van contactgegevens of indirecte gegevens als IP adres etc.. Openbaar worden van gegevens leidt tot weinig of geen schade.
P = L / 1	Privacy gevoeligheid Laag: Het betreft alleen beperkte persoonsgegevens nodig voor het proces. Bijvoorbeeld: contactgegevens interne medewerkers, email adres t.b.v. workflow of logging, etc. Openbaar worden van gegevens leidt tot weinig of geen schade.
P = B / 0	Niet van toepassing: Er worden geen Persoonsgegevens verwerkt.

Hulpvragen + opmerkingen		B	L	M	H
A	PIA proces op hoofdlijnen • Identificeer de (nieuwe) verwerking van onder meer persoonsgegevens welke te beoordelen is en beschrijf deze op hoofdlijnen (verwerkingsregister niveau) • Toets het privacy risico a.d.h.v. de 10 Criteria voor risicobepaling ➔ Vaststellen PIA noodzaak • Indien PIA niet noodzakelijk: • Vastleggen van de besluitvorming, geautoriseerd door de PO/FG • Indien PIA noodzakelijk: • Inrichten van een multidisciplinair PIA team en uitvoeren PIA conform PIA procesbeschrijving. • Doorvoeren van de geïdentificeerde maatregelen in de verdere realisatie van de verwerking.				
B	Criteria voor bepaling Privacy risico Is er sprake van: 1. Beoordelen van mensen op basis van persoonskenmerken (profiling)? 2. Geautomatiseerde besluitvorming met rechtsgevolgen voor betrokkene? 3. Stelselmatige en grootschalige monitoring (b.v. cameratoezicht)? 4. Gevoelige / bijzondere persoonsgegevens? 5. Grootschalige gegevensverwerking? 6. Matching of samenvoeging van datasets? 7. Gegevens over kwetsbare personen? 8. Innovatief gebruik of toepassing van nieuwe technologieën? 9. Blokkering van een recht, dienst of contract? 10. Grensoverschrijdend verkeer van persoonsgegevens naar buiten de EU? Indien 2 of meer criteria van toepassing dan zeker een PIA uitvoeren.				
C	Impact van risicobepaling: De classificatie heeft gevolgen in termen van maatregelen welke genomen dienen te worden om het risico te beperken: • H: Uitvoeren van PIA, waarin passende maatregelen dienen te worden gedefinieerd om de vastgestelde risico's te mitigeren. De maatregelen volgen dus uit het PIA onderzoek en worden ook vastgelegd in het Verwerkingsregister. • M: Borgen van Privacy by Design en Privacy by Default in het implementatie proces. Tevens dient dit proces opgenomen te worden in het Verwerkingsregister • L: Vanwege het beperkte karakter zijn er in principe geen aanvullende maatregelen benodigd. Een vastlegging in het verwerkingsregister is ook niet verplicht. • B: Maatregelen nvt.				
Geef de motivatie hoe je tot de keuze gekomen bent. Dit is vooral belangrijk voor toekomstig gebruik 					
Totaal, cumulatief. Vul hier de hoogste waarde in voor Privacy					

P* = **M**