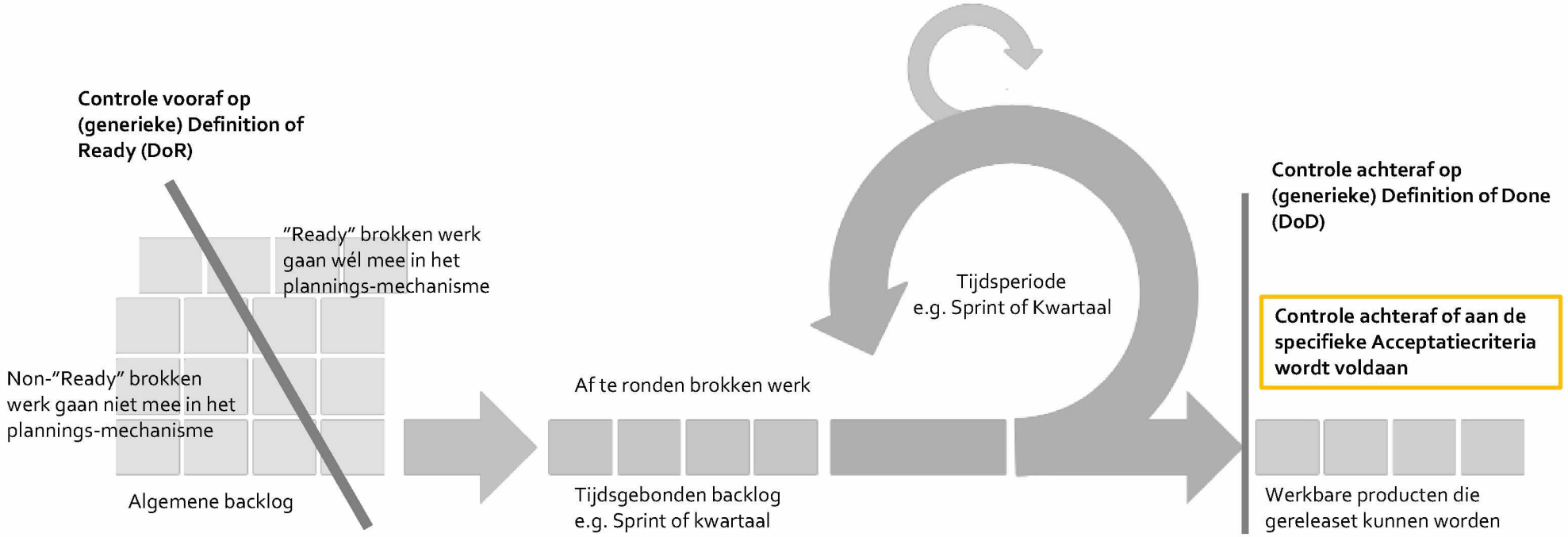
Quality Assurance Acceptatiecriteria v1.0



	Definition of Ready (DoR)	Definition of Done (DoD)	Acceptatiecriteria
Definitie	Criteria waaraan het werk moet voldoen *voordat het opgepakt/gepland* kan worden	Criteria waaraan het werk moet voldoen *voordat het opgeleverd* kan worden	Criteria waaraan het werk moet voldoen *voordat het 'af' is en in productie kan worden genomen*

#	Vraag	Ja/ Nee	Acceptatiecriteria[1]	Korte toelichting op de vraag
1.	**Verandert er iets in de Architectuur?**	Ja	**PSA of Architectuurnotitie** (in te vullen door Architect) **is opgesteld en afgestemd met de Architect.**	De Project Start Architectuur (PSA) is een projectdocument dat zich richt op kaders die op het project van toepassing zijn en die impact hebben op essentiële structuurkeuzes die in het project gemaakt moeten worden. De PSA beschrijft globaal – in hoofdstructuren - wat de start en de gewenste eindsituatie zijn van het project ten aanzien van organisatie-, proces-, informatie-, applicatie- en technologie-inrichting.
		Nee	Geen	
2.	**Wordt er gebruik gemaakt van gegevens die in de basis- en kernregistraties beschikbaar is?**	Ja	**Er wordt voldaan aan de aansluitvoorwaarden met basisinformatie die in overleg met de Data-Office zijn vastgesteld.**	Als een bestuursorgaan bij het vervullen van zijn publiekrechtelijke taak een gegeven nodig heeft dat in de basis- en kernregistraties beschikbaar is, mag het dit gegeven niet meer uitvragen. Dan hoeft een burger of bedrijf dit gegeven niet vaker aan te leveren dan nodig. Zo dalen de administratieve lasten. Als een bestuursorgaan bij het vervullen van zijn publiekrechtelijke taak een gegeven nodig heeft dat in de basis- en kernregistraties beschikbaar is, dan moet het dit gegeven gebruiken uit de basis- en kernregistraties. Zo is wettelijk geborgd dat al deze personen en organisaties werken met dezelfde kwalitatieve gegevens. Gegevens in de basis- en kernregistraties zijn: • Administratieve kadastrale gegevens • Kadastrale kaarten • Kleinschalige Kaarten • Grootschalige Kaarten • Gebieden • Bedrijven, Stichtingen, Verenigingen, ZZP-ers, Scholen, Kerken • Adressen en Gebouwen • Voertuigen • Inkomen en vermogen • Monumenten • WKPB beperkingen • Persoonsgegevens (van NAW tot en met bijzondere persoonsgegevens) • Panoramabeelden
		Nee	Geen	

[1] In de kolom acceptatiecriteria staan instrumenten en acties die gebruikt c.q. uitgevoerd moeten worden om de voor Quality Assurance noodzakelijke maatregelen te identificeren en te adresseren.

				• Waarde onroerende zaken • Luchtfoto's • Hoogtebestanden • Ondergrond • Peilmerken • Meetbouten De Data-Office adviseert over de wijze van gebruik van de basis- en kernregistratie en geeft inzicht in de van toepassing zijnde aansluitvoorwaarden.
3.	**Is er sprake van een of meer van de onderstaande vijf omstandigheden?** 1. Nieuw beleid of regelgeving dat/die betrekking hebben op verwerking van persoonsgegeven of waaruit verwerkingen van persoonsgegeven voortvloeien 2. Verwerking op grote schaal van bijzondere persoonsgegevens of persoonsgegevens met betrekking tot strafrechtelijke veroordelingen en strafbare feiten en/of BSN 3. Grootschalige en stelselmatige observatie of monitoring 4. Er wordt gebruik gemaakt van profilering of systematische en uitgebreide analyse van persoonlijk aspecten, en daaraan zijn voor betrokkenen rechtsgevolgen verbonden 5. Een risicovolle verwerking	Ja	**Data Protection Impact Assessment (DPIA) is uitgevoerd en eventuele aanvullende maatregelen zijn afgestemd met de Privacy Officer.**	Bijzondere persoonsgegevens zijn gegevens die iets zeggen over: • Ras of etnische afkomst • Politieke opvattingen • Lidmaatschap vakbond • Religieuze of levensbeschouwelijke overtuigingen • Genetische en/of biometrische gegevens • Gezondheidsgegevens • Gegevens over seksueel gedrag of seksuele gerichtheid • BSN • Strafrechtelijke gegevens Er is sprake van een risicovolle verwerking indien twee of meer van de volgende aspecten aan de orde zijn: • Er worden persoonsgegevens gebruikt om betrokkenen te evalueren/scoren. • Geautomatiseerde besluitvorming met rechtsgevolg of vergelijkbaar wezenlijk gevolg • Stelselmatige monitoring • Er worden gevoelige gegevens of gegevens van zeer persoonlijke aard verwerkt • Er vindt gegevensverwerking plaats op grote schaal • Er worden datasets gecombineerd of gematched • Er worden gegevens verwerkt van kwetsbare groepen betrokkenen • Er worden nieuwe technologieën gebruikt die mogelijk een bedreiging vormen voor privacy
		Nee	Geen	

				• Er is door de verwerking sprake van het ontnemen/beperken van de rechten van betrokkenen, of is de verwerking een voorwaarde voor een dienst
4.	**Is er een wettelijke grondslag waarop persoonsgegevens verwerkt worden?**	Ja	**De wettelijke grondslag waarop persoonsgegevens worden verwerkt is vastgesteld, beschreven en afgestemd met de Privacy Officer.**	Om persoonsgegevens te mogen verwerken moet je een wettelijke basis hebben, of wel wettelijke grondslag in AVG termen. De verwerking van de persoonsgegevens moet op een van de wettelijke grondslagen kunnen worden gebaseerd. Als het gaat om een taak van algemeen belang/publieke taak of een wettelijke verplichting, dient dit te worden aangevuld met sectorale wet- en regelgeving (en ook beleid indien van toepassing). Als er een wettelijke grondslag is, dan moet aan de eisen uit bijvoorbeeld de AVG voldaan worden en zijn maatregelen nodig (bv. dataminimalisatie of niet meer verzamelen dan nodig). Dit zijn de mogelijke wettelijke grondslagen uit art 6 AVG: 1. Toestemming 2. Uitvoering overeenkomst 3. Vitaal belang 4. Wettelijke verplichting 5. Taak algemeen belang / uitoefening openbaar gezag 6. Gerechtvaardigd belang Als er geen wettelijke grondslag is, dan mogen persoonsgegevens niet verwerkt worden.
		Nee	**Met de Privacy Officer is besloten hoe het initiatief toch door kan gaan zonder verwerking van persoonsgegevens.**	
5.	**Zijn alle persoonsgegevens die in het proces worden gebruikt ook daadwerkelijk noodzakelijk voor het proces?**	Ja	Geen	Het beginsel van dataminimalisatie vloeit voort uit artikel 5 van de AVG en geeft aan dat persoonsgegevens alleen verwerkt mogen worden als dit strikt noodzakelijk is. Uit dit beginsel vloeit ook voort dat persoonsgegevens alleen mogen worden verwerkt indien het doel van de verwerking niet redelijkerwijs op een andere wijze kan worden verwezenlijkt, bijvoorbeeld met geaggregeerde gegevens. <u>Praktische toets</u>, kan je bij elk persoonsgegeven aangeven waarom het proces niet goed uitgevoerd kan worden zonder dat persoonsgegeven. Als dat niet aangegeven kan worden, dan wordt niet voldaan aan het uitgangspunt van dataminimalisatie. <u>Aanvullend</u>, denk na of je niet met minder persoonsgegevens toe kan.
		Nee	**Alleen noodzakelijke persoonsgegevens mogen gebruikt worden, dataminimalisatie is uitgevoerd en afgestemd met de Privacy Officer.**	

6.	**Is de kring van personen waarvan de persoonsgegevens wordt verwerkt in kaart gebracht en beschreven?**	Ja	**De kring van personen over wie persoonsgegevens wordt verwerkt is in kaart gebracht, vastgelegd en afgestemd met de Privacy Officer.**	Degene van wie persoonsgegevens worden verwerkt, worden in de AVG 'betrokkenen' genoemd. Betrokkenen hebben bepaalde rechten, zoals inzage in hun persoonsgegevens en om correctie en verwijdering kunnen vragen. Voor betrokkenen uit kwetsbare groepen kunnen aanvullende rechten of zwaardere privacy eisen gelden. Voorbeelden van kwetsbare betrokkenen: minderjarigen, anders validen, mensen met schulden, asielzoekers, etnische minderheden, zieken.
		Nee	Geen	
7.	**Is er sprake van een verwerker van persoonsgegevens?**	Ja	**Verwerkersovereenkomst is goedgekeurd door Privacy Officer en afgesloten met derde(n) partij(en).**	Wordt er met een externe partij gewerkt, dan kan het zijn dat deze externe partij een verwerker is. Een verwerker is een instantie/orgaan die persoonsgegevens verwerkt in opdracht van de verwerkingsverantwoordelijke (in dit geval de Gemeente Amsterdam) waarbij de verwerkingsverantwoordelijke het doel en de middelen bepaalt. Is er sprake van een verwerker, dan moet er een verwerkersovereenkomst worden afgesloten. Een verwerkersovereenkomst wordt gesloten als een externe organisatie/leverancier persoonsgegevens verwerkt of gebruikt in opdracht van de gemeente en de gemeente verwerkingsverantwoordelijke blijft (zeggenschap houdt) over deze gegevens. De verwerker moet de (Quality Assurance) instructies van de gemeente opvolgen, zodat de verwerker net zo zorgvuldig met de gegevens omgaat als de gemeente. In de verwerkersovereenkomst worden afspraken gemaakt over hoe er met deze persoonsgegevens wordt omgegaan. Het gemeentelijk model voor de verwerkersovereenkomst kan je hier vinden: Afspraken met derden - Intranet Amsterdam
		Nee	Geen	
8.	**Worden er persoonsgegevens verwerkt buiten de Europese Economische Ruimte (EER)?**	Ja	**Data Transfer Assessment (DTA) is opgesteld en afgestemd met de Privacy Officer.**	De gemeente hanteert het beleid om zo min mogelijk gebruik te maken van (sub)verwerkers buiten de EER. Als er sprake is van doorgifte van persoonsgegevens naar een land buiten de EER (en er voor dat land geen adequaatheidsbesluit is genomen), dient een Data Transfer Assessment (DTA) te worden uitgevoerd. Hieruit zal moeten blijken dat de persoonsgegevens voldoende worden beschermd. Onder het kopje "Afspraken voor het verwerken van persoonsgegevens buiten de EER" kan je het format door de DTA vinden en informatie over het verwerken van persoonsgegevens buiten de EER in relatie tot de AVG: Afspraken met derden - Intranet Amsterdam
		Nee	Geen	

9.	**Is het (openbaarheid) classificatieniveau van de informatie voortkomend uit het proces bepaald?**	Ja	Geen	Classificeren is het proces van toekennen van het classificatieniveau van informatieobjecten, waarin de mate van openbaarheid c.q. vertrouwelijkheid wordt afgewogen. De afweging vindt plaats op basis van het beleidskader 'classificatie van informatieobjecten'. Het resultaat van dit proces is het classificatieniveau dat in de metadata bij het informatieobject wordt vastgelegd. Informatie kan als openbaar, vertrouwelijk of geheim worden geclassificeerd. Om naar de gemeentelijke openbaarheidsambitie en wet- en regelgeving te handelen streven we ernaar om zoveel mogelijk informatie als openbaar te classificeren. Het toekennen van de vertrouwelijke of geheime classificatie kan alleen als er een wettelijke grondslag is, moet worden beargumenteerd en is voor een bepaalde termijn. Meer informatie is hier te vinden: Classificeren van informatie - Intranet Amsterdam
		Nee	**Classificatieniveau van informatie is bepaald en afgestemd met Adviseur Informatiebeheer en Information Security Officer.**	
10.	**Vindt er in het kader van een nieuw proces/taak opslag of registratie van data/documenten plaats? M.a.w. is sprake van een nieuwe informatiestroom/registratie?**	Ja	**Met adviseur informatiebeheer de bewaartermijn van informatie vastgesteld en vervolgacties afgesproken.**	Wanneer een nieuw proces of nieuwe taak uitgevoerd gaat worden, brengt dat opslag en registratie van nieuwe data/documenten met zich mee. Het proces of de taak moet worden beschreven. Hierbij moet de bewaartermijn vastgesteld worden, mogelijk ook zaaktypes (voor standaardisatie dossiervorming) uitgewerkt worden en de benodigde (beheer-)metadata moeten kunnen worden toegekend. Afhankelijk van het soort proces en de bijbehorende bewaartermijn, zijn er meer of minder maatregelen te treffen.
		Nee	Geen	
11.	**Wordt er een nieuwe applicatie geïmplementeerd? Of is er een "major release" van een bestaande applicatie? Of gaat het om een vitaal proces?**	Ja	**Privacy, Informatiebeheer & Informatiebeveiliging eisen zijn opgenomen in Programma van Eisen (bij een aanbesteding) en/of bij ontwerp en inrichting. Tevens is er een technische beveiligingsaudit ("pentest") uitgevoerd en vervolgstappen zijn afgestemd met de Information Security Officer.**	Wanneer er een nieuwe applicatie aangeschaft/gebruikt gaat worden, moet privacy, opslag, registratie en beveiliging van data en documenten (by design) worden ingericht. Afhankelijk van het soort proces zijn er enkele maatregelen te treffen. Een penetratietest of pentest is een toets van een of meer computersystemen op kwetsbaarheden, waarbij deze kwetsbaarheden ook werkelijk gebruikt worden om in deze systemen in te breken. Overige vereiste analyses en documentatie (te bespreken met de adviseur informatiebeheer): Functioneel ontwerp, procesbeschrijving(en), vastgestelde bewaartermijnen, metadatering, zaaktypes, bewaring en vernietiging ingericht (on premise) of regelen dat het wordt ingericht (SaaS).
		Nee	Geen	

12.	**Wordt er binnen het proces volledig digitaal gewerkt?**	Ja	Geen	De gemeente werkt volledig digitaal. Toch zijn er ook nog papieren documenten in omloop. Dit komt omdat de organisatie post ontvangt en brieven uitprint om handmatig te ondertekenen. Om dat papier te vervangen door digitale bestanden is een handboek vervanging en Besluit tot vervanging nodig. Bij het in gebruik nemen van een nieuwe applicatie of anderszins kan het ook zijn dat een bestaand handboek vervanging geactualiseerd moet worden. Het handboek Vervanging bestaat bijvoorbeeld uit het uitwerken van de procedure van scanning, het inrichten van het scanproces, kwaliteitsborging scan, etc.
		Nee	**De papieren stromen zijn gedigitaliseerd. Het proces hieromtrent is in een handboek Vervanging uitgewerkt en afgestemd met Adviseur Informatiebeheer en er is een Besluit Vervanging genomen door desbetreffende directeur.**	
13.	**Indien er al volledig digitaal gewerkt wordt, is er sprake van een Handboek Vervanging dat geactualiseerd moet worden?**	Ja	**Het Handboek Vervanging is geactualiseerd en aangepast naar de nieuwe situatie ingevuld en afgestemd met de Adviseur Informatiebeheer.**	Een Handboek Vervanging (en Besluit Vervanging) moet bij wijzigingen van bepaalde orde geactualiseerd worden. Indien deze epic/feature bijdraagt aan zulke wijzigingen is het van belang een bestaand handboek met de daarin opgenomen procedures en werkafspraken over digitalisering van papieren informatiestromen te actualiseren.
		Nee	Geen	
14.	**Wordt er digitale informatie gemigreerd en/of geconverteerd?**	Ja	**Migratieplan & Migratieverslag zijn opgesteld en afgestemd met de Adviseur Informatiebeheer en Verklaring van Migratie is ondertekend door verantwoordelijke directeur.**	Moet digitale informatie overgezet van de ene omgeving naar de andere omgeving of in een ander formaat worden gezet? Dit komt vaak voor wanneer een bestaande voorziening wordt vervangen door iets anders. Migraties/conversies van informatie moeten worden gedocumenteerd in een Migratieplan en Migratieverslag, waaruit blijkt dat geen onacceptabel informatieverlies is opgetreden, en dat de latende omgeving is opgeruimd. Op basis daarvan ondertekent de directeur de Verklaring van Migratie waarin dit formeel wordt bevestigd, conform artikel 25 lid 2 van de Archiefregeling 2014.
		Nee	Geen	
15.	**Wordt er informatie vernietigd?**	Ja	**Vernietigingsprocedure is opgesteld en afgestemd met de Adviseur Informatiebeheer, door de verantwoordelijke directeur is een machtiging vernietiging (incidenteel of doorlopend) aangevraagd bij & verleend door het Stadsarchief.**	Vernietiging van informatie uit een bepaalde omgeving kan eenmalig zijn of terugkerend. Daarvoor moet een incidentele respectievelijk doorlopende machtiging van de gemeentearchivaris worden verkregen. De wijze waarop de vernietiging plaatsvindt moet procedureel worden beschreven en daarna worden vastgesteld door de directeur. Van de te vernietigen informatie moeten overzichten worden gemaakt, en als de vernietiging is uitgevoerd moet daar bewijs van worden geleverd in een rapportage. Van uitgevoerde vernietigingen moet opgave worden gedaan bij de gemeentearchivaris.
		Nee	Geen	
16.	**Wordt er een applicatie uitgefaseerd?**	Ja	**Uitfaseringsplan hoe met data wordt omgegaan is opgesteld en**	Het beheer van informatie in een applicatie die buiten gebruik wordt gesteld,

			afgestemd met de Adviseur Informatiebeheer.	moet worden geregeld. Informatie waarvan de bewaartermijn is verstreken moet worden vernietigd, overige informatie moet worden gearchiveerd/gemigreerd (zie verder de vorige twee punten).
		Nee	Geen	
17.	**Wordt er informatie overgebracht naar het Stadsarchief Amsterdam?**	Ja	**Protocol van Overbrenging is opgesteld en afgestemd met de Adviseur Informatiebeheer.**	Een klein deel van de informatie mag nooit worden vernietigd, en moet na verloop van de archiefwettelijke termijn (nu 20 jaar, wordt 10 jaar) worden overgebracht naar Stadsarchief Amsterdam (E-depot). Op uiterlijk het moment van overbrenging moet de informatie voldoen aan de standaarden die Stadsarchief Amsterdam oplegt m.b.t. metadatering en bestandsformaten. Protocol van Overbrenging bevat onder andere metadatering conform standaard (TMLO/MDTO), Bestandsformaten (conversie naar verplichte formaten)
		Nee	Geen	
18.	**Wordt er informatie overgebracht van of naar een andere organisatie (vervreemding, uitlening, ter beschikking stelling)?**	Ja	**Verklaring van vervreemding/uitlening/ter beschikking stelling en documentatie behorend bij migratie en/of vernietiging is opgesteld en afgestemd met de Adviseur Informatiebeheer.**	Informatie kan tijdelijk of permanent in of uit beheer worden gegeven, o.a. door het overnemen of afstoten van een (wettelijke) taak. Hiervan worden verklaringen opgemaakt en ondertekend door de betreffende directeuren/diensthoofden. Hier zal vaak ook migratie een rol spelen; zie het eerdere punt daarover.
		Nee	Geen	
19.	**Wordt er informatie gecreëerd en opgeslagen welke valt onder één of meer informatiecategorieën die actief openbaar gemaakt dienen te worden? Of wordt er met informatie gewerkt waarvan de doelgroep (burger/ondernemer/bezoeker/ journalistiek) de behoefte heeft dat de informatie actief openbaar wordt gemaakt (inspanningsverplichting)?**	Ja	**Er is een publicatieproces ingericht conform de handreiking 'openbaarheid by design' en afgestemd met het projectteam 'Open Tenzij'**	De 11 verplichte Wet open overheid (Woo) categorieën die de overheid actief openbaar moet maken: - Wet- en Regelgeving - Organisatiegegevens - Raadstukken - Bestuurstukken - Stukken van Adviescolleges - Convenanten - Jaarplannen en -verslagen - Wob/Informatieverzoeken - Onderzoeken - Beschikkingen - Klachten Als het antwoord 'ja' is dan zal tijdens het project de mogelijkheid tot actieve openbaarmaking via publicatiekanaal gerealiseerd moeten worden.
		Nee	Geen	

				Bijvoorbeeld een koppeling tussen applicatie en publicatiekanaal of een handmatige procesinrichting. Naast de 11 verplichte informatiecategorieën geldt o.b.v. art 3.1 van de Woo een inspanningsverplichting. De organisatie maakt bij uitvoering van haar taak uit eigen beweging de documenten voor eenieder openbaar, indien dit zonder onevenredige inspanning of kosten redelijkerwijs mogelijk is. Het doel is proactief aan de informatiebehoefte van de burger te voldoen. De handreiking 'openbaarheid by design' wordt momenteel ontwikkeld. Neem voor meer informatie contact op met het projectteam 'Open Tenzij' van de vakgroep Openbaarheid en Informatiebeheer.
20.	**Is het basisbeveiligingsniveau (BBN) van het proces bepaald?**	Ja	**Implementatie maatregelen volgend uit BIO Quickscan bepaald met de Information Security Officer.**	Om te bepalen of een proces, informatiesysteem en/of informatie een bepaald Basis Beveiligings Niveau (BBN) heeft binnen de BIO. De uitkomsten kunnen dan worden gebruikt om te bepalen of er meer maatregelen nodig zijn voor een proces en onderliggende informatiesystemen. Het resultaat van de BIO Quickscan kan duiden op een zwaartepunt in het te beschermen belang. Bijvoorbeeld door een hogere score voor vertrouwelijkheid maar niet op Integriteit en beschikbaarheid.
		Nee	**BIO Quickscan uitgevoerd en implementatie maatregelen bepaald met de Information Security Officer.**	
21.	**Betreft het een toepassing die aan burgers, ondernemers of bezoekers beschikbaar wordt gesteld?**	Ja	**Striktere informatiebeveiliging is nodig, autorisatieproces is bepaald & afgestemd met de Information Security Officer**	Een toepassing die aan burgers, ondernemers of bezoekers beschikbaar wordt gesteld kan bijvoorbeeld een webapplicatie zijn die met bijzondere persoonsgegevens werkt of als DigiD gebruikt wordt.
		Nee	Geen	
22.	**Vindt de hosting van het (informatie)systeem plaats bij 1 van de bestaande partijen (SaaS leverancier, KPN, of elders)?**	Ja	Geen	Bij bestaande partijen kan het zijn dat de huidige afspraken ook geldig zijn voor deze epic/feature. Bij nieuwe partijen zullen er eisen gesteld moeten worden aan deze partijen.
		Nee	**Informatiebeveiliging eisen zijn bepaald & afgestemd met de Information Security Officer, leverancier en directie Digitale Voorzieningen**	
23.	**Omvat de epic/feature een toepassing waarbij koppelingen met andere (informatie)systemen nodig zijn?**	Ja	**Beveiligde verbindingen met de andere (informatie)systemen zijn bepaald & afgestemd met de Information Security Officer**	TLS beschermt de communicatie tussen een client en een server. Het beschermen van communicatie is vooral belangrijk als er gevoelige informatie via een verbinding wordt verstuurd. Informatie kan gevoelig zijn vanwege de vertrouwelijkheid (zoals inloggegevens) en vanwege de integriteit (zoals een financiële
		Nee	Geen	

				transactie).
24.	**Is beschikbaarheid van de toepassing van belang (beschikbaarheid tussen of op bepaalde tijden)?**	Ja	**Maatregelen die de noodzakelijke beschikbaarheid garanderen zijn bepaald en afgestemd met de Information Security Officer**	Denk hier bijvoorbeeld na over de maximale tijd dat de toepassing niet beschikbaar mag zijn. Beschikbaarheid en maximale uitval i.r.t. het BBN niveau, komt expliciet aan bod in de BIO Quickscan.
		Nee	Geen	
25.	**Is de juistheid (integriteit) van de gegevens van de toepassing van belang?**	Ja	**Integriteitseisen zijn bepaald en afgestemd met de Information Security Officer**	De juistheid (integriteit) van gegevens houdt in dat informatie actueel is en geen fouten bezit. Hierbij kun je denken aan veranderingen in data die altijd geautoriseerd worden uitgevoerd. Als dit niet het geval is, wordt de integriteit van data in gevaar gebracht en is het minder goed beschermd. M.a.w. integriteit van gegevens houdt in dat deze juist, actueel en volledig zijn.
		Nee	Geen	
26.	**Is toegang tot de gegevens van het (informatie)systeem / het proces van belang ?**	Ja	**Autorisatiematrix (toegang & functiescheiding) is bepaald en afgestemd met de Information Security Officer**	Logische toegangsbeveiliging zorgt er voor dat onbevoegden minder makkelijk toegang kunnen krijgen tot gemeentelijke informatiesystemen en de informatie binnen deze gemeentelijke informatiesystemen. Door het ontbreken van adequate logische toegangsbeveiliging (waaronder een goede autorisatie matrix) bestaat het risico dat onbevoegden zich toegang kunnen verschaffen tot (de informatie binnen) gemeentelijke informatiesystemen, waardoor ongewenste acties op de diensten kunnen plaatsvinden en/of informatie kan worden ontvreemd of verminkt.
		Nee	Geen	
27.	**Zijn een of meerdere onderstaande statements van toepassing?** a. Er wordt nieuwe technologie gebruikt. b. 'Mensenwerk' wordt deels gedigitaliseerd of geautomatiseerd. c. Er is een hoge impact naar buiten toe, voor de stad en inwoners. d. Er is sprake van profilering van personen of gebieden. e. Er is sprake van gericht sturen/beïnvloeden van gedrag.	Ja	**Ethische bijsluiter is ingevuld en up-to-date en workshop 'Introductie TADA-waarden' is gevolgd door Epic Owner/ Product Owner/B-lead/I-lead**	Om bij het gebruik van technologie de morele waarden van de gemeente Amsterdam en daarmee de digitale rechten van de Amsterdammers te waarborgen, is een multidisciplinaire afweging voor, tijdens en na de realisatie gewenst. Onverwachte ongewenste negatieve gevolgen moeten voorkomen worden en gemaakte keuzes moeten altijd uitgelegd kunnen worden aan de Amsterdamse burgers, ondernemers en bezoekers, de media en het bestuur. De ethische bijsluiter maakt de waarden en dilemma's van teams expliciet. Hierdoor kan het team rekening houden met de rechten, belangen en wensen van alle betrokkenen. Dankzij de Ethische bijsluiter kan een team deze afwegingen transparant maken en uitleggen richting burgers, raadsleden en belanghebbenden. De epic-owner moet ervoor zorgen dat voor de epic de ethische bijsluiter wordt gemaakt & toegepast als één van de statements in de lijst van toepassing is. De ethische bijsluiter is een instrument dat:
		Nee	Geen	

	f. Er worden voorspellende data-analyses gedaan. g. Er wordt gebruik gemaakt van (gedeeltelijk) geautomatiseerde besluitvorming. h. Een specifieke doelgroep ondervindt mogelijk verhoogd ongemak. i. Onderbuikgevoel: 'Dit kan ik niet met droge ogen uitleggen.' j. Kans op stigmatisering of versterking van ongelijkheid tussen groepen/plekken. k. Gevolgen zijn mogelijk ingrijpend op lange termijn of nog onduidelijk. **l.** Uit de Data Protection Impact Assessment (DPIA) blijkt dat er sprake is van risicovolle verwerking van persoonsgegevens.			– Inzicht geeft in de positieve effecten en negatieve ethische bijwerkingen van de voorgenomen digitalisering. – In staat stelt te bepalen of het moreel verantwoord is om door te gaan met de epic. – In staat stelt maatregelen voor de Definition of Ready en Definition of Done te formuleren voor de features om positieve effecten te vergroten en de negatieve bijwerkingen te verkleinen. *Zowel de introworkshop als begeleiding bij de ethische bijsluiter vraag je aan door te mailen naar* 5.1,2,e *@amsterdam.nl en* 5.1,2,e *@amsterdam.nl*