Stadsbank Oost Nederland

Procedure melden van incidenten

Maatregelen BIG die met de procedure worden onderbouwd:

Hoofdstuk 13: Beheer van incidenten

1.Doelstelling

Conform de BIG hanteert de Stadsbank de volgende doelstellingen:

- Informatiebeveiligingsgebeurtenissen behoren zo snel mogelijk te worden gerapporteerd.
- De procedure voorziet in de gestructureerde en vastgelegde werkwijze voor het melden en registreren van (bijna) incidenten.
- Waar een vervolgprocedure tegen een persoon of organisatie na een informatiebeveiligingsincident juridische maatregelen omvat (civiel of strafrechtelijk), behoort bewijsmateriaal te worden verzameld, bewaard en gepresenteerd overeenkomstig de voorschriften voor bewijs die voor het relevante rechtsgebied zijn vastgelegd.

2. Implementatie

a) Er is een procedure voor het rapporteren van beveiligingsgebeurtenissen vastgesteld, waarin de handelingen worden vastgelegd die moeten worden genomen na het ontvangen van een beveiligingsincident.

b) Het rapporteren van beveiligingsincidenten vindt plaats aan de Security Officer. In geval van een mogelijk datalek wordt de Functionaris Gegevensbescherming bij de afhandeling van het incident betrokken.

c) Alle beveiligingsincidenten worden door de SO vastgelegd in Topdesk.

d) Alle relevante beveiligingsincidenten kunnen worden geëscaleerd aan de Informatiebeveiligingsdienst (= IBD) van KING.

e) Datalekken worden door de SO gemeld bij de Functionaris Gegevensbescherming. Deze bepaalt of melding plaatsvindt aan de AP en/of aan de betrokken burgers.

f) Vermissing of diefstal van apparatuur of media die gegevens van de Stadsbank kunnen bevatten, wordt altijd aangemerkt als informatiebeveiligingsincident.

g) Informatie over de beveiligingsrelevante handelingen, bijvoorbeeld loggegevens, foutieve inlogpogingen, van de gebruiker wordt regelmatig nagekeken. De Security Officer bekijkt periodiek – bij voorkeur maandelijks - een samenvatting van de informatie.

h) Voor een vervolgprocedure naar aanleiding van een beveiligingsincident behoort bewijsmateriaal te worden verzameld, bewaard en gepresenteerd overeenkomstig de voorschriften voor bewijs die voor het relevante rechtsgebied zijn vastgelegd.

3.Bekendmaking

De inhoud van deze procedure moet bekend zijn bij alle medewerkers van de Stadsbank. Dit geldt dus ook voor de extern ingehuurde medewerkers.

4.Definities

Beveiligingsincident:

iedere gebeurtenis die schade toebrengt of kan toebrengen aan de beveiliging van informatie. Hiermee wordt bedoeld iedere inbreuk op het gebied van beschikbaarheid, betrouwbaarheid, vertrouwelijkheid en/of controleerbaarheid, een inbreuk op de beveiliging van persoonsgegevens.

Datalek: beveiligingsincident dat leidt tot de aanzienlijke kans op ernstige nadelige gevolgen dan wel ernstige nadelige gevolgen heeft voor de bescherming van persoonsgegevens.

Melding:
Melding aan IBD of kennisgeving van een datalek aan de Autoriteit Persoonsgegevens (AP en/of aan de betrokkene.
Mogelijke incidenten zijn o.a.:

- Uitlekken van gevoelige informatie zoals een kwijtgeraakte USB stick per persoonsgegevens;
- Bedreiging of intimidatie (extern of intern);
- Onbevoegde aanwezigheid;
- Diefstal met of zonder geweld;
- Interne fraude;
- Diefstal met of zonder braak;
- Verdacht postpakket;
- Fraude door de klant;
- (Hack) exploit;
- Verstoring van de beschikbaarheid van IT systemen
- Calamiteiten zoals brand in de serverruimte.

6. Meldplicht Datalekken

Sinds 1 januari 2016 is de wet Meldplicht Datalekken van kracht. Met de invoering van deze wet wordt beoogd om de gevolgen van een datalek voor de burger zoveel mogelijk te beperken en hiermee een bijdrage te leveren aan het behoud en herstel van vertrouwen in de omgang met persoonsgegevens.

6.1 Wanneer melden?

Wanneer technische en organisatorische beveiligingsmaatregelen niet hebben gefunctioneerd, wordt hiervan melding gedaan. Persoonsgegevens zijn dan blootgesteld aan een aanmerkelijke kans op onbedoelde of onwettige vernietiging, verlies of onrechtmatige wijziging van, of een niet geautoriseerde toegang tot persoonsgegevens.
Het moet gaan om *ernstige nadelige* gevolgen voor de betrokkene, als gevolg van een beveiligingsprobleem. De aard en omvang van het lekken speelt dus een belangrijke rol.
Een inbreuk op de beveiliging hoeft niet te betekenen dat beveiligingsmaatregelen niet voldoende zijn. Gegevens kunnen bijvoorbeeld ook in verkeerde handen zijn gevallen door bijvoorbeeld diefstal van een computer, laptop of tablet. Het kan ook gaan om menselijke fouten; denk bijvoorbeeld aan het verzenden van gevoelige gegevens naar een onjuist e-mailadres zonder versleuteling. In al deze gevallen dient de Stadsbank bij de Autoriteit Persoonsgegevens melding te doen van een datalek. Deze melding vindt plaats door de Functionaris Gegevensbescherming.

6.2 Bestuurlijke boete

De meldplicht houdt in, dat de Stadsbank als verantwoordelijke melding moet maken van inbreuken op de beveiliging met ernstige nadelige gevolgen voor de bescherming van persoonsgegevens of inbreuken die leiden tot een aanzienlijke kans daarop. De melding moet gedaan worden bij de Autoriteit Persoonsgegevens en eventueel

ook aan betrokkene(n). Dit in geval de inbreuk waarschijnlijk ongunstige gevolgen zal hebben voor diens persoonlijke levenssfeer. De melding moet het volgende bevatten:

- de aard van de inbreuk
- de instanties waar meer informatie over de inbreuk kan worden verkregen
- een beschrijving van de geconstateerde en de vermoedelijke gevolgen van de inbreuk voor de verwerking van persoonsgegevens
- de maatregelen die de organisatie heeft genomen of voorstelt te nemen om deze gevolgen te verhelpen

6.Prioritering van incidenten

De prioriteit van een incident wordt meestal bepaald door de beoordeling van de impact en urgentie, waarbij:

- Urgentie de maat is voor hoe snel de oplossing van het incident vereist is.
- Impact de maat is voor de omvang van het incident en van de mogelijke schade als gevolg van het incident voordat het kan worden opgelost.

6.1 Urgentie van incidenten

In de linker kolom van onderstaande tabel worden urgentie categorieën beschreven. De urgentie van een incident wordt vastgesteld door de van toepassing zijnde waarde van de desbetreffende categorie te kiezen op basis van de bij de omschrijving vermelde oorzaken van het incident. De urgentie wordt bepaald door één of een combinatie van de genoemde oorzaken.

Categorie	Omschrijving van de urgentie
Hoog (H)	▪ De schade veroorzaakt door het incident neemt snel toe. ▪ Werk dat moet worden hersteld door personeel is zeer arbeidsintensief. ▪ Een groot incident kan worden voorkomen door bij een klein incident onmiddellijk te handelen.
Medium (M)	▪ De schade veroorzaakt door het incident neemt in de tijd aanzienlijk toe. ▪ Er gaat werk verloren, maar dit is relatief snel te herstellen.
Laag (L)	▪ De schade veroorzaakt door het incident neemt in de tijd maar weinig toe. ▪ Het werk dat blijft liggen is niet tijdsintensief.

6.2 Impact van het incident

Om de impact van het incident vast te stellen, wordt de van toepassing zijnde incident impact categorie gekozen. De impact wordt bepaald door één of een combinatie van de genoemde oorzaken.

Categorie	Omschrijving
Hoog (H)	▪ Relatief veel personeel is geraakt door het incident en/of kan zijn/haar werk niet meer doen. Meerdere organisatie onderdelen zijn geraakt. ▪ Burgers of bedrijven zijn geraakt en/of lijden schade, op welke wijze dan ook, als gevolg van het incident. Persoonsgegevens zijn gecompromitteerd (datalek melden). ▪ De financiële impact van het incident is hoger dan €10.000,-. ▪ Er is reputatie schade, de krant wordt gehaald. ▪ Er zijn lichamelijk gewonden.
Medium (M)	▪ Enig personeel is geraakt door het incident en/of kan zijn/haar werk niet meer doen, bijvoorbeeld een afdeling. ▪ Enkele inwoners zijn geraakt en/of lijden schade, op welke wijze dan ook, als gevolg van het incident. Persoonsgegevens zijn gecompromitteerd maar de schade kan snel worden gerepareerd. ▪ De financiële impact van het incident is hoger dan €1.000,- en lager dan €10.000,-. ▪ Er is kans op reputatie schade.
Laag (L)	▪ Enkele personeelsleden zijn geraakt door het incident en/of kunnen niet meer hun werk doen. ▪ Enkele burgers zijn minimaal geraakt en/of lijden minimale schade. ▪ De financiële impact van het incident is lager dan €1.000,- ▪ Er is geen kans op reputatie schade.

6.3 Incident Prioriteiten Matrix

Als er klassen zijn gedefinieerd om urgentie en impact in te schalen, dan kan een *Incident Prioriteit Matrix* gebruikt worden om prioriteringsklassen te herleiden. In het onderstaande voorbeeld zijn de klassen uitgewerkt met een code en kleuren.

		Impact		
		Hoog	Midden	Laag
Urgentie	Hoog	1	2	3
	Midden	2	3	4
	Laag	3	4	5

Code/kleur	Omschrijving	Reactietijd	Oplossingstijd
1	Kritiek	Onmiddellijk	1 uur
2	Hoog	10 minuten	4 uur
3	Medium	1 uur	8 uur
4	Laag	4 uur	24 uur
5	Zeer laag	1 dag	1 week

6.4 Verantwoordelijkheid

De verantwoordelijkheid voor deze procedure ligt te allen tijde bij het MT van de Stadsbank en namens deze bij de security officer.

6.5 Proceseigenaar

De proceseigenaar is het afdelingshoofd Bedrijfsvoering en Advies.

6.6 Actualiteit

De proceseigenaar is verantwoordelijk voor het actueel houden van deze procedure. Als de procedure inhoudelijk wijzigt, draagt de proceseigenaar zorg voor communicatie daarover en distributie en archivering van de procedure.

6.7 Uitvoering

1.
Elke medewerker van de Stadsbank (en door de Stadsbank ingeschakelde bewerkers) is verplicht een vermoedelijk beveiligingsincident te melden aan de security officer. Melder meldt via telefoon en email, de SO verwerkt de melding in Topdesk.

2.
De medewerkers zijn eveneens verplicht zwakke plekken in de beveiliging (of het vermoeden daarvan) te melden aan de security officer. Een dergelijke verplichting is erop gericht tekortkomingen in de beveiliging zo snel mogelijk te ontdekken en te kunnen oplossen.

3.
De medewerkers zijn eveneens verplicht onvolkomenheden in de programmatuur (of vermoeden daarvan) op het terrein van beveiliging te melden aan de security officer. Een dergelijke verplichting is erop gericht onvolkomenheden in de programmatuur zo snel mogelijk te ontdekken en te kunnen oplossen.

4.
Door de security officer wordt het (bijna) incident geregistreerd in Topdesk.

5.
Door de security officer wordt vervolgens het incident onderzocht als 1e lijns.

Bij dit onderzoek wordt aandacht besteed aan de volgende aspecten:

- Wat is de aard en urgentie van het incident;
- Wat is de impact van het incident;
- Welke systemen zijn betrokken;
- Wat is de oorzaak dat dit incident heeft plaatsgevonden;
- Is er sprake van het niet nakomen van of een tekortkoming in de beveiligingsprocedures;
- Is een eventuele tekortkoming in de beveiliging hersteld;
- Kan dit incident nogmaals optreden;
- Welke acties moeten worden getroffen om herhaling te voorkomen.

Bij dit onderzoek wordt de melder betrokken. De bevindingen worden vastgelegd bij registratie van het incident in Topdesk.

6.
Door de security officer wordt onmiddellijk de urgentie bepaald van het gemelde incident aan de hand van de in deze procedure opgenomen urgentietabel. De urgentie wordt geregistreerd in Topdesk.
Bij een hoge urgentie wordt meteen contact gezocht met het IST.

7.
Tegelijk wordt door de security officer onmiddellijk de vermoedelijke impact bepaald aan de hand van de in deze procedure opgenomen impacttabel.

8.
Aan de hand van de ernst van het incident wordt de prioriteit bepaald.

9.
Bij incidenten met een hoge urgentie en/of grote impact wordt de manager Bedrijfsvoering en Advies en de CISO ingeschakeld door de security officer . Zij bepalen gezamenlijk of het IST bijeen moet komen en welke agendaleden hierbij moeten aansluiten.
De security officer neemt tevens direct maatregelen om bewijsmateriaal en andere gegevens die in dit stadium als relevant worden beschouwd, veilig te stellen.

10.
De security officer stelt van het onderzoek een verslag op en rapporteert dit aan de betrokken leidinggevenden. Tevens wordt de melder geïnformeerd over de uitkomsten van het onderzoek.

11.
Relevante zaken worden door security officer intern gemeld aan het IST en extern in geval van incidenten met een hoge urgentie en/of grote impact via de landelijke opschaling aan de IBD → NCSC en in geval van *ernstige* compromittering van persoonsgegevens aan de Autoriteit Persoonsgegevens. Samen met de directeur wordt bepaald hoe naar het publiek wordt gecommuniceerd.

12.
Informatie over de beveiligingsrelevante handelingen, bijvoorbeeld loggegevens, foutieve inlogpogingen, van de gebruiker wordt regelmatig nagekeken. De security officer bekijkt periodiek een samenvatting van de informatie. Zowel de meldingen als de wijze van afhandeling worden in Topdesk opgenomen. De CISO legt het incident vast in de managementrapportage aan de directie.

13.
Voor een eventuele vervolging naar aanleiding van een beveiligingsincident behoort bewijsmateriaal te worden verzameld, bewaard en – na aangifte- te worden gepresenteerd aan het Openbaar Ministerie.

14.
Bij een (vermoed) incident is de bewaartermijn van de verzamelde gegevens minimaal drie jaar.

Beheersmaatregel:	13.1.1
Documentversie:	1.0 12 maart 2018
Documentnaam:	180312 Procedure melden van incidenten

Stadsbank
Oost Nederland

Voorstel

Aan:	Dagelijks Bestuur
Van:	Directeur
Datum:	12 april 2018
Betreft:	Informatiebeveiligingsbeleid Stadsbank Oost Nederland 2018

Te besluiten:

1. Kennis te nemen van het Informatiebeveiligingsbeleid Stadsbank Oost Nederland 2018;
2. Het Informatiebeveiligingsbeleid Stadsbank Oost Nederland 2018 vast te stellen.

Privacy is een grondrecht. De bescherming van de persoonlijke levenssfeer is vastgelegd in het Europees Verdrag inzake de rechten van de mens en de fundamentele vrijheden (EVRM) en in de Grondwet. De Wet bescherming persoonsgegevens (Wbp) is de Nederlandse wet die bescherming van dit grondrecht regelt en uitwerkt. Per 25 mei 2018 wordt de Wbp vervangen door de AVG, de Algemene Verordening Gegevensbescherming. Deze verordening heeft rechtstreekse werking in alle lidstaten van de Europese Unie en zorgt voor een uniforme regelgeving voor de bescherming van persoonsgegevens binnen de Unie. Een aantal specifieke regels, bijvoorbeeld over het gebruik van het Burger Service Nummer, is verder uitgewerkt in een uitvoeringswet AVG.

Uitwerking van maatregelen vindt plaats op basis van de Baseline Informatiebeveiliging Gemeenten (BIG). Gemeentelijke overheden hebben zich geconformeerd aan de implementatie van een basisniveau van informatiebeveiliging voor 2018. Hoewel het geen wettelijke verplichting betreft, geldt er wel een bindende afspraak tussen gemeenten en gemeentelijke samenwerkingsverbanden om de informatiebeveiliging conform de BIG te implementeren. Stadsbank Oost Nederland wil zich als Gemeenschappelijke Regeling hieraan ook conformeren.

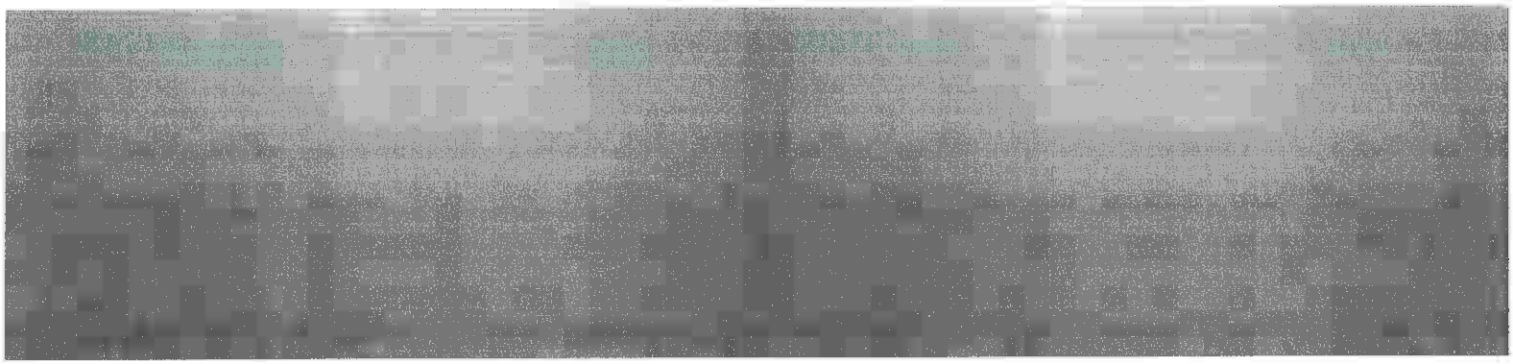
Hiertoe is bijgaand informatiebeveilingsbeleid opgesteld, dat conform de BIG door het Dagelijks Bestuur moet worden vastgesteld. Het informatiebeveiligingsbeleid is van toepassing op alle processen van de Stadsbank, de onderliggende informatiesystemen, informatie en (persoons)gegevens van de Stadsbank en externe partijen (gemeenten, klanten, leveranciers) en het gebruik van deze systemen, processen en informatie door medewerkers en (keten)partners in de meest brede zin van het woord. In dit beleid wordt aangegeven hoe de Stadsbank intern de bescherming van de gegevens van haar cliënten, medewerkers en bedrijfsvoering regelt. Het geeft aan hoe persoonsgegevens moeten worden verwerkt en welke kaders en uitgangspunten de organisatie daarbij hanteert. Daarnaast wordt aangegeven op welke wijze het beleid in de organisatie wordt geborgd en

hoe we de opslag en het beheer van de persoonsgegevens geregeld hebben. Het beleid vormt de grondslag voor de verdere uitwerking van fysieke, organisatorische en technische maatregelen.

Het informatiebeveiligingsbeleid wordt in de planning & control cyclus eenmaal per 4 jaar geëvalueerd en aan het Dagelijks Bestuur ter vaststelling aangeboden. Jaarlijks wordt van de uitvoering het beleid verslag gedaan in een separate paragraaf in het jaarverslag.

Bijlage:

- Informatiebeveiligingsbeleid SON (versie 2018).



Stadsbank
Oost Nederland

INFORMATIEBEVEILIGINGSBELEID STADSBANK OOST NEDERLAND

Versie 2018

Inhoud

1. Inleiding

In dit beleid wordt aangegeven hoe de Stadsbank Oost Nederland intern de bescherming van de gegevens van haar cliënten, medewerkers en bedrijfsvoering regelt. Het geeft aan hoe persoonsgegevens moeten worden verwerkt en welke kaders en uitgangspunten de organisatie daarbij hanteert. Daarnaast wordt aangegeven op welke wijze het beleid in de organisatie wordt geborgd en hoe we de opslag en het beheer van de persoonsgegevens geregeld hebben. Het beleid vormt de grondslag voor de verdere uitwerking van fysieke, organisatorische en technische maatregelen. Daarbij is specifieke aandacht noodzakelijk voor de zwakste schakel in de informatieveiligheidsketen: de mens. Medewerkers moeten in het kader van informatieveiligheid bewust bekwaam worden gemaakt. Dit beleid is daarom ook de basis voor het inzicht van elke medewerker in zijn/haar rol in het bereiken en behouden van gegevensbescherming c.q. informatiebeveiliging.

Reikwijdte van het beleid

Het informatiebeveiligingsbeleid is van toepassing op alle processen van de Stadsbank, de onderliggende informatiesystemen, informatie en (persoons)gegevens van de Stadsbank en externe partijen (gemeenten, klanten, leveranciers) en het gebruik van deze systemen, processen en informatie door medewerkers en (keten)partners in de meest brede zin van het woord, ongeacht locatie, tijdstip en gebruikte apparatuur.

Juridisch kader

Privacy is een grondrecht. De bescherming van de persoonlijke levenssfeer is vastgelegd in het Europees Verdrag inzake de rechten van de mens en de fundamentele vrijheden (EVRM) en in de Grondwet. De Wet bescherming persoonsgegevens (Wbp) is de Nederlandse wet die bescherming van dit grondrecht regelt en uitwerkt. Per 25 mei 2018 wordt de Wbp vervangen door de AVG, de Algemene Verordening Gegevensbescherming. Deze verordening heeft rechtstreekse werking in alle lidstaten van de Europese Unie en zorgt voor een uniforme regelgeving voor de bescherming van persoonsgegevens binnen de Unie. Een aantal specifieke regels, bijvoorbeeld over het gebruik van het Burger Service Nummer, is verder uitgewerkt in een uitvoeringswet AVG.

Uitwerking van maatregelen vindt plaats op basis van de Baseline Informatiebeveiliging Gemeenten (BIG). Gemeentelijke overheden hebben zich geconformeerd aan de implementatie van een basisniveau van informatiebeveiliging voor 2018. Hoewel het geen wettelijke verplichting betreft, geldt er wel een bindende afspraak tussen gemeenten om de informatiebeveiliging conform de BIG te implementeren.

2. Algemene uitgangspunten gegevensbescherming

De basis voor de (gegevensbescherming door de) AVG wordt gevormd door een aantal uitgangspunten. Deze uitgangspunten zijn in de jaren tachtig van de vorige eeuw vastgelegd door de Organisatie voor Economische Samenwerking en Ontwikkeling (OESO). Het gaat om de volgende principes:

- Rechtmatige grondslag

  Persoonsgegevens mogen uitsluitend worden verwerkt op basis van de limitatieve grondslagen zoals die in de AVG zijn vastgelegd. Deze gronden zijn een expliciete toestemming van betrokkenen, een overeenkomst, een wettelijke verplichting, een vitaal belang, een publieke taak of een gerechtvaardigd belang. Soms kunnen deze gronden strijdig zijn. Zo kan een verwerking op grond van een taak van algemeen belang (een rechtmatige grondslag) tegelijkertijd een inbreuk maken op de privacy van een individu. Dan moet per geval een afweging worden gemaakt tussen de privacybescherming van betrokkene(n) en het maatschappelijk belang.

- Transparantie

  Personen dienen te worden geïnformeerd over het gebruik van hun persoonsgegevens en over de daarbij gebruikte (technologische) middelen. Ook dient de persoon daarover controle uit te kunnen uitoefenen en dient hij/zij een verwerking in rechte te kunnen aanvechten. Om te kunnen voldoen aan het principe van transparantie is het nodig dat de volledige datastroom, de architectuur en inrichting van de verwerkingen inzichtelijk is (volledig gedocumenteerd). Dit geldt ook als de verwerkingen zijn uitbesteed aan een derde. Daarnaast moet duidelijk en controleerbaar zijn welke medewerkers toegang hebben tot welke systemen.

- Doelbinding

  Persoonsgegevens worden alleen voor vooraf welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden verzameld en mogen daarna niet verder worden verwerkt als dat onverenigbaar is met de doeleinden. Van elke verwerking moet dus een specifieke en beperkte doelstelling zijn vastgelegd. Met het doel wordt duidelijk waarvoor de gegevens mogen worden gebruikt en – misschien nog wel belangrijker – ook waarvoor ze niet mogen worden gebruikt.

- Gegevensminimalisatie

  Alleen persoonsgegevens die toereikend zijn, ter zake dienend en beperkt tot wat noodzakelijk is voor de verwerkingsdoeleinden mogen worden verwerkt. Met andere woorden: alleen de voor het doel strikt noodzakelijke gegevens worden verzameld. Hierbij zijn vragen relevant als "kan het doel van de verwerking ook op een andere, minder privacy-belastende wijze bereikt worden, met minder data?" (in een ontwerpfase is dit onderdeel van het 'Privacy by Design'-principe). Daarnaast worden gegevens niet onnodig verspreid en dienen de gegevens enkel toegankelijk te zijn voor medewerkers die de gegevens nodig hebben voor hun functie.

- Juistheid

  Verwerkte persoonsgegevens moeten juist zijn en blijven en dus moeten ze (bijvoorbeeld op verzoek van betrokkene) zo nodig worden geactualiseerd. Alle redelijke maatregelen moeten worden genomen om de persoonsgegevens die onjuist zijn, direct te wissen of te verbeteren. Of gegevens onjuist zijn hangt mede af van de doeleinden waarvoor zij worden verwerkt. Met dit principe wordt onder andere geborgd dat er geen fout of vertekend beeld van een betrokkene ontstaat.

- Opslagbeperking

  Persoonsgegevens mogen niet langer bewaard worden dan voor het specifieke doel noodzakelijk is. Met andere woorden: persoonsgegevens moeten worden vernietigd zodra dat mogelijk is. Een organisatie dient aannemelijk te kunnen maken dat gegevens kunnen worden gewist en dat deze in specifieke situaties ook werkelijk zijn gewist. Voor gegevens van kwetsbare groepen zoals kinderen, kan het noodzakelijk zijn om deze met prioriteit te wissen. Alleen voor archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden kunnen uitzonderingen gelden, mits er passende technische en organisatorische maatregelen worden getroffen.

- Integriteit en vertrouwelijkheid

  Persoonsgegevens moeten beschermd worden tegen toegang/inzage door onbevoegden, (on)opzettelijk verlies, vernietiging of beschadiging. Hiervoor moeten passende technische en organisatorische beveiligingsmaatregelen worden getroffen. Bij het bepalen wat 'passend' is, zijn de risico's van de verwerking leidend en het beveiligingsniveau moet daarop zijn afgestemd. Daarbij moet rekening worden gehouden met de stand van de techniek, de uitvoeringskosten en de aard, omvang, context en doeleinden van de verwerking.

- Verantwoordingsplicht (accountability)

  Een persoon of organisatie die verantwoordelijk is voor een verwerking toont aan dat er maatregelen zijn genomen om privacy risico's uit te bannen of te beperken. Deze concrete maatregelen en procedures hebben betrekking op alle niveaus in de organisatie (strategisch, tactisch en operationeel). Vervolgens moet ook worden getoetst en aangetoond (bijvoorbeeld door interne of externe audits) of de maatregelen in de praktijk voldoende zijn. Om deze verantwoording te kunnen doen moet er inzicht zijn in alle verwerkingen, de daarbij gebruikte technologie en de risico's daarvan.

3. Persoonsgegevens

Wat zijn persoonsgegevens?

Elk gegeven dat betrekking heeft op een natuurlijke persoon (betrokkene) is een persoonsgegeven. Om van een persoonsgegeven te spreken is het voldoende dat de betrokkene met de binnen de organisatie vastgelegde gegevens identificeerbaar is. Gegevens waarmee dit rechtstreeks kan zijn bijvoorbeeld de NAW-gegevens, maar het kan ook via indirecte gegevens zoals een paspoortnummer of een IP-adres. Andere voorbeelden van persoonsgegevens zijn: e-mailadressen, telefoonnummers, geslacht, huwelijkse staat, familie en beroep.

Bijzondere en strafrechtelijke gegevens

Een speciale categorie van persoonsgegevens zijn bijzondere persoonsgegevens. Het gaat dan bijvoorbeeld om medische of gezondheidsgegevens. Dit type persoonsgegevens is door de wetgever extra beschermd. Er geldt een verbod op het verwerken van bijzondere persoonsgegevens tenzij daarvoor een zwaarwegend belang of wettelijke grondslag aanwezig is. Een andere speciale categorie zijn strafrechtelijke gegevens. Deze mogen alleen worden verwerkt onder toezicht van de overheid of als dat uitdrukkelijk in een wet is toegestaan. Voor Nederland wordt dat geregeld in de Uitvoeringswet AVG. Voor de Stadsbank is het nog relevant dat het verwerken van strafrechtelijke gegevens ook is toegestaan door en ten behoeve van publiekrechtelijke samenwerkingsverbanden als dat noodzakelijk is voor de uitvoering van hun taak. Voorwaarde daarbij is dat er zodanige waarborgen zijn dat de persoonlijke levenssfeer van de betrokkene niet onevenredig wordt geschaad.
Voor deze beide categorieën van persoonsgegevens gelden zwaardere eisen voor de beveiliging van de gegevens. Denk bijvoorbeeld aan het direct verwijderen van deze gegevens na uitvoering van de taak waarvoor ze verzameld zijn.

Persoonsgegevens van gevoelige aard

Verwerkingen van gegevens die kunnen leiden tot discriminatie, identiteitsdiefstal of -fraude, financiële verliezen, reputatieschade of enig ander aanzienlijk economisch of maatschappelijk nadeel, en verwerkingen van persoonsgegevens van kwetsbare natuurlijke personen, met name van kinderen, worden gezien als persoonsgegevens van gevoelige aard. Ook deze moeten specifieke bescherming krijgen.

Verwerken van persoonsgegevens

De AVG maakt onderscheid tussen een 'verwerkingsverantwoordelijke' en een 'verwerker. Een organisatie is verwerkingsverantwoordelijke als zij het *doel en de middelen* voor de verwerking vaststelt. Een verwerker is de persoon of instantie die *ten behoeve van* de verwerkingsverantwoordelijke persoonsgegevens verwerkt. Een verwerker heeft zelf geen doel bij de verwerking en dient de instructies van de verantwoordelijke op te volgen.

De Stadsbank vervult haar dienstverlening namens 22 gemeenten op basis van een gemeenschappelijke regeling, waarin zij is aangewezen als een openbaar lichaam met

een zelfstandige rechtspersoonlijkheid. De Stadsbank verzamelt de voor haar dienstverlening benodigde persoonsgegevens zelfstandig en onttrekt deze gegevens niet aan de gemeentelijke basisregistraties. De Stadsbank bepaalt welke persoonsgegevens worden verwerkt en met welk doel en bepaalt ook of derden toegang krijgen tot de persoonsgegevens en wanneer deze worden gewist.

Het uitgangspunt van dit informatiebeveiligingsbeleid is dat de Stadsbank wordt beschouwd als 'verwerkingsverantwoordelijke' en niet als 'verwerker'. Voor de opslag van persoonsgegevens wordt door de Stadsbank gebruik gemaakt van derden. Deze derden worden beschouwd als verwerkers van gegevens ten behoeve van de Stadsbank. Met deze organisaties sluit de Stadsbank als verwerkingsverantwoordelijke verwerkersovereenkomsten. Het gaat hierbij om grootschalige verwerkingen van geautomatiseerde aard.

De Stadsbank maakt voor de uitvoering van haar taken ook gebruik van personen en instanties (bijvoorbeeld bewindvoerders, gerechtsdeurwaarders), die vanuit de Stadsbank persoonsgegevens verstrekt krijgen. Hierbij gaat het om kleinschalige verwerkingen. In correspondentie met deze derden wordt de vertrouwelijkheid van de verstrekte persoonsgegevens benadrukt. Daarnaast wordt de cliënt in het op de website van de Stadsbank gepubliceerde privacy-statement op de hoogte gesteld van de mogelijkheid van deze verwerking.

Omgaan met persoonsgegevens

Alle verwerkingen van persoonsgegevens die door of namens de Stadsbank plaatsvinden, zijn vastgelegd in een register van verwerkingen. In dit register is per verwerkingsactiviteit aangegeven:

- De naam en contactgegevens van de verwerkingsverantwoordelijke en de FG;
- De doeleinden voor gegevensverwerking;
- Een beschrijving van de categorieën betrokkenen en categorieën persoonsgegevens;
- De (voorgenomen) categorieën ontvangers;
- De (voorgenomen) bewaartermijnen, en;
- Een algemene beschrijving van de beveiligingsmaatregelen.

Het register wordt bijgehouden door de Functionaris Gegevensbescherming, die namens de Autoriteit Persoonsgegevens toezicht houdt op de gegevensverwerkingen.

Bij verwerking van persoonsgegevens is een aantal fasen te onderscheiden, namelijk de verzameling, de opslag, het gebruik en de verwijdering van deze gegevens.

<u>Verzameling van persoonsgegevens</u>

Verzameling van gegevens vindt uitsluitend plaats op basis van de in de AVG genoemde grondslagen voor een rechtmatige gegevensverwerking. Alleen de voor het doel strikt noodzakelijke gegevens worden verzameld. In het privacy-statement op de website van de Stadsbank is aangegeven welke persoonsgegevens worden verwerkt.

Opslag van persoonsgegevens

De Stadsbank heeft de opslag van de persoonsgegevens uitbesteed aan derden. Voor het borgen van een passende beveiliging van de gegevens worden met deze derden verwerkersovereenkomsten gesloten, zoals in de vorige paragraaf is aangegeven. Hierbij wordt aangesloten op de door de VNG overeenkomstig de GIBIT-voorwaarden opgestelde modelovereenkomst. In deze overeenkomsten worden waarborgen voor de beschikbaarheid, integriteit en vertrouwelijkheid van de persoonsgegevens vastgelegd. Met de ondertekening van de verwerkersovereenkomst garandeert de verwerker dat de verwerking op een adequate wijze wordt beschermd door het treffen van beveiligingsmaatregelen. Zowel bij opslag als verzending van gegevens (via e-mail of internet) wordt versleuteling (encryptie) toegepast.

Gebruik van persoonsgegevens

De toegang tot persoonsgegevens is voorbehouden aan medewerkers die hiertoe geautoriseerd zijn op basis van hun uit te voeren taken. Het raadplegen, muteren en verwijderen van gegevens vindt plaats op basis van individuele autorisaties. Voorafgaand aan autorisatie vindt identificatie en authenticatie van medewerkers plaats met behulp van gebruikersnaam en wachtwoord. Medewerkers worden in de gedragscode gewezen op hun verantwoordelijkheden bij de beveiliging van persoonsgegevens.

Verwijdering en archivering van persoonsgegevens

Persoonsgegevens mogen niet langer worden bewaard dan voor het specifieke doel van de verwerking noodzakelijk is. Dat betekent dat zij moeten worden verwijderd zodra dat mogelijk is. De bewaartermijn van de persoonsgegevens per verwerking is vastgelegd in het register van verwerkingsactiviteiten. Als uitgangspunt voor de vaststelling van de bewaartermijn wordt rekening gehouden met de Archiefwet. Door een combinatie van technische en organisatorische maatregelen wordt gewaarborgd dat persoonsgegevens tijdig worden gewist. Bij archivering kan pseudonimisering of anonimisering worden toegepast. Bij pseudonimisering is sprake van een omkeerbare versleuteling, bij anonimisering zijn de persoonsgegevens niet meer herleidbaar naar hun oorspronkelijke vorm.

4. Inrichting van de beveiligingsorganisatie

Verantwoordelijkheden

Het Dagelijks Bestuur is integraal verantwoordelijk voor de beveiliging (beslissende rol) van informatie binnen de werkprocessen van de Stadsbank en stelt de kaders voor informatiebeveiliging en gegevensbescherming vast op basis van landelijke en Europese wet- en regelgeving en normenkaders op het gebied van informatieveiligheid;

De directie (in een sturende rol) is verantwoordelijk voor kaderstelling en sturing:

- stuurt op organisatiebrede risico's;
- controleert of de getroffen maatregelen overeenstemmen met de betrouwbaarheidseisen en of deze voldoende bescherming bieden;
- draagt zorg voor de formele inrichting van de beveiligingsorganisatie en de aanwijzing van FG, SO en CISO;
- evalueert periodiek beleidskaders en stelt deze waar nodig bij.

De managers in de lijn zijn verantwoordelijk voor de integrale beveiliging van hun organisatieonderdelen en processen, het sturen op beveiligingsbewustzijn en de naleving van regels en richtlijnen (gedrag en risicobewustzijn).

Het intern samengestelde Informatie Security Team (IST) is in een coördinerende rol verantwoordelijk voor uitvoering van het IB-beleid:

- stelt op basis van een expliciete risicoafweging betrouwbaarheidseisen voor de informatiesystemen op;
- is verantwoordelijk voor beveiliging van de informatievoorziening en implementatie van beveiligingsmaatregelen;
- is verantwoordelijk voor alle beheeraspecten van informatiebeveiliging, zoals bescherming persoonsgegevens (volgens WBP, AVG), ICT-security management en cybercriminaliteit, meldplicht datalekken, facilitaire en personele zaken en incident en problem management;
- verzorgt logging, monitoring en interne/externe rapportage.

Taken en rollen

- Het Dagelijks Bestuur stelt formeel het Informatiebeveiligingsbeleid (IB-beleid) vast.
- De directie adviseert het Dagelijks Bestuur formeel over het vast te stellen IB-beleid.
- De directie en management dragen zorg voor de kaderstelling, sturing, bewustwording en borging van het IB-beleid in de organisatie.
- De monitoring van IB-taken is belegd bij het Informatie Security Team (IST). Het IST treedt ook op als crisisteam voor de informatiebeveiliging.
- De manager Bedrijfsvoering & Advies is voorzitter van het IST-team.
- De Chief Information Security Officer (CISO) coördineert de IB-taken en adviseert - namens het IST - de directie, het management en het Dagelijks Bestuur gevraagd en ongevraagd over het IB-beleid. Gezien de aard en omvang van de organisatie van de Stadsbank worden de taken van de CISO gekoppeld aan de bestaande functie van senior-adviseur P&C. De CISO is voor zijn coördinerende en adviserende taken onafhankelijk van de lijnorganisatie gepositioneerd.

- De uitvoering van technische maatregelen en het toezicht op deze maatregelen, voor zover uitvoering plaatsvindt door derden, is belegd bij de Security Officer (SO).
- Het toezicht op de (rechtmatigheid van de) gegevensverwerkingen vindt plaats door de Functionaris Gegevensbescherming (FG).
- De lijnmanagers zijn als proceseigenaar verantwoordelijk voor de binnen hun afdeling uitgevoerde processen. De manager Bedrijfsvoering & Advies is verantwoordelijk voor de bedrijfsondersteunende processen.
- Binnen de lijnorganisatie worden door de lijnmanagers medewerkers benoemd die als aanspreekpunt fungeren voor SO en FG.
- Het kernteam van het IST bestaat uit:
  - Chief Information Security Officer (CISO);
  - Functionaris Gegevensbescherming (FG);
  - Concern controller (bedrijfscontinuïteit);
  - Security Officer (SO).

Naar behoefte en noodzaak kan het kernteam worden uitgebreid met de volgende personen. Zij zijn agendalid van het kernteam IST:

- de managers schulddienstverlening en beschermingsbewind (proceseigenaar), bepalen beveiligingseisen, bewustwording en borging in primaire proces);
- één klantmanager met coördinerende taken (bewustwording en borging in primaire proces);
- coördinator kredietverstrekking (bewustwording en borging bij kredietverstrekking en telefoonverkeer met klanten);
- adviseur P&O;
- adviseur bedrijfsprocessen;
- functioneel applicatiebeheerder;
- adviseur facilitaire zaken;
- medewerker communicatie.

Per onderdeel van het IB-beleid wordt een trekker aangewezen uit het IST-team.

Het IST-team stelt een informatiebeveiligingsplan op, in overleg met de managers schulddienstverlening, beschermingsbewind en Bedrijfsvoering & Advies voor hun onderdelen, en stelt dit eenmaal per 4 jaar bij of vaker, indien nodig. Over de voortgang wordt gerapporteerd aan de CISO en in het IST. Aan elke beveiligingsmaatregel is een actiehouder gekoppeld. De actiehouder ziet toe op de implementatie van de maatregelen in de lijnorganisatie. De verantwoordelijkheid voor het treffen van de beveiligingsmaatregelen berust bij de eigenaar van het te beveiligen proces, dus bij de lijnmanager. De status van de maatregelen wordt vastgelegd in het ISMS-systeem en bewaakt door de CISO.

Over het functioneren van informatiebeveiliging wordt door de CISO jaarlijks gerapporteerd conform de P&C cyclus (begroting en jaarrekening) en in voorkomende gevallen bij het optreden van incidenten en/of problemen.

De medewerker communicatie verzorgt de interne en externe communicatie rondom informatiebeveiliging, beveiligingsincidenten en -problemen, in afstemming met de CISO, FG en de directie.

De Ondernemingsraad van de Stadsbank wordt door het kernteam vroegtijdig betrokken bij en geïnformeerd over zaken, die betrekking hebben op het personeel van de Stadsbank en instemmings- of adviesrecht met zich meebrengen.

Functioneel overleg

De CISO organiseert tenminste drie keer per jaar een (security) overleg met het IST. De manager Bedrijfsvoering & Advies is voorzitter. Het overleg richt zich met name op de voortgang van de uitvoering van het beleid, advisering over tactisch/strategische informatiebeveiliging kwesties en mogelijke testen in de informatiebeveiliging.

Het onderwerp informatiebeveiliging dient verder een vast onderdeel te zijn op de agenda van afdelings- en team-overleggen, zodat er sturing plaatsvindt op de uitgevoerde activiteiten en bewustwording bij de medewerkers wordt bevorderd. Hiervoor zijn de managers verantwoordelijk.

Externe partijen

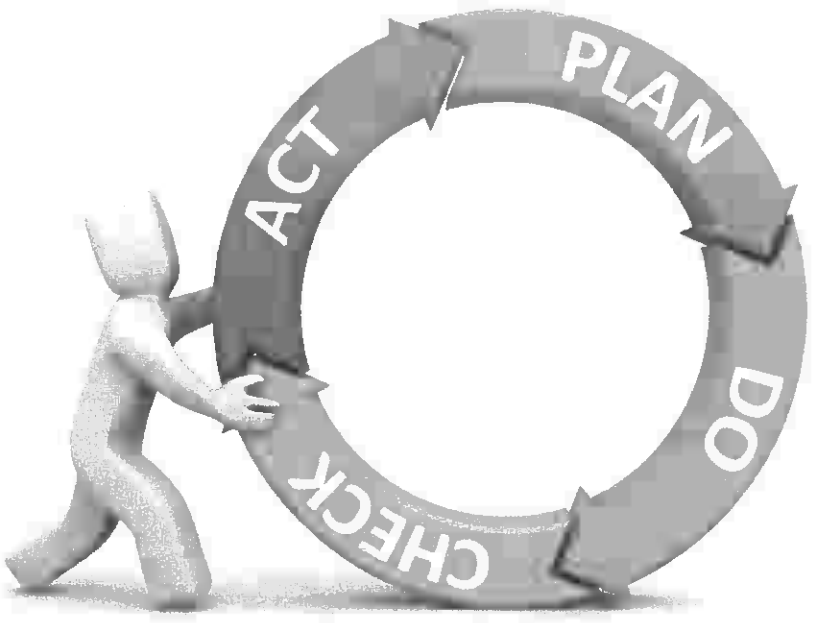
IB-beleid, landelijke normen en wet- en regelgeving gelden ook voor externe partijen (gemeenten, leveranciers, (keten)partners) waarmee de Stadsbank samenwerkt (en informatie mee uitwisselt). Hierbij geldt het 'comply or explain' beginsel (pas toe of leg uit).

Overeenkomsten met derden dienen te worden getoetst aan het IB-beleid. Indien noodzakelijk worden vereiste beveiligingsmaatregelen aanvullend vastgelegd. In de verwerkersovereenkomsten met leveranciers is onder meer geborgd dat beveiligingsincidenten onmiddellijk worden gerapporteerd en dat de Stadsbank het recht heeft afspraken te (laten) controleren.

Voor het tot stand brengen van datakoppelingen en externe hosting van data en/of services met externe partijen is het IB-beleid van toepassing, met name gericht op risicobeheersing.

PDCA

Informatiebeveiliging is een continu verbeterproces. 'Plan, do, check en act' vormen samen het management systeem van informatiebeveiliging. Deze kwaliteitscyclus is onderstaand weergegeven:



- Plan: De cyclus start met de planning van de uitvoering van het IB-beleid. Planning geschiedt op jaarlijkse basis.
- Do: Het beleidskader is de basis voor risicomanagement, uitvoering van (technische) maatregelen en bevordering van beveiligingsbewustzijn. Uitvoering geschiedt op dagelijkse basis en maakt integraal onderdeel uit van het werkproces.
- Check: Control is onderdeel van het werkproces met als doel: waarborgen van de kwaliteit van informatie, (persoons)gegevens, ICT, en compliance aan wet- en regelgeving. Externe controle vindt plaats buiten het primaire proces door een auditor (accountant, ICT-diensten).
- Act: De cyclus is rond met de uitvoering van verbeteracties o.b.v. check en externe controle.

De cyclus is een continu proces; de bevindingen van controles zijn weer input voor de jaarplanning en beveiligingsplannen. De bevindingen worden in beginsel gerapporteerd in de P&C cyclus. Voor ingrijpende verbeteracties wordt een gevraagde beslissing voorgelegd aan het MT.

5. Bewustwording en communicatie

Op alle niveaus in de organisatie moet het belang van bescherming van persoonsgegevens duidelijk zijn en worden gedragen. Iedereen in de organisatie moet op de hoogte zijn van de nieuwe privacyregels en het belang van gegevensbescherming voor de organisatie.

Om tot een gezamenlijk niveau van bewustwording en kennis te komen, zijn inmiddels afspraken gemaakt met een organisatie die de Stadsbank gaat ondersteunen bij het op een aansprekende manier stimuleren van de bewustwording. Dit vindt plaats door middel van de inzet van een *mystery guest, telefonische misleiding* en het verzenden van *phishing-mails*. De resultaten van deze acties worden aan de medewerkers teruggekoppeld tijdens een bankbijeenkomst. Hoe we verder het belang van gegevensbescherming op een goede (ludieke) manier blijvend onder de aandacht brengen, is onderwerp van het communicatieplan dat door de communicatieadviseur wordt opgesteld.

Strategisch niveau

Op het niveau van directie/bestuur is de voornaamste rol het ondersteunen van de bewustwording het vaststellen van dit beleid en het formeel vaststellen van de beveiligingsorganisatie, zoals deze hiervoor beschreven is. Daarnaast dient op dit niveau de impact van mogelijke risico's voor de organisatie ingeschat te worden en worden hier besluiten genomen over de maatregelen die nodig zijn en over het al dan niet accepteren van risico's. De directie heeft in dit verband de verantwoordelijkheid voor de keuzes die het managementteam (MT) in dit verband maakt. Directie verantwoordt de keuzes van het MT naar het bestuur. Ook heeft de directie een belangrijke rol in het zorgen dat er bij besluiten over de bedrijfsvoering expliciet aandacht is voor de bescherming van persoonsgegevens en dat overwegingen en keuzes daaromtrent worden vastgelegd. Het standaard uitvoeren van een *PIA* voorafgaand aan beslissingen over (nieuwe) gegevensverwerkingen wordt hierbij als instrument ingezet.

Tactisch niveau

Bij het MT moet vooral de vertaling van het beleid naar de uitvoering plaatsvinden. Er moet worden ingeschat wat de impact van de BIG en de AVG is op de huidige processen, producten en diensten en welke aanpassingen in de uitvoering nodig zijn om aan de verplichtingen te voldoen. Medewerkers moeten worden geïnformeerd via trainingen en workshops en via praktische werkinstructies en handleidingen. Regelmatige aandacht voor het belang van gegevensbescherming tijdens werkoverleggen draagt bij aan een blijvende bewustwording. Het MT heeft verder een rol in het creëren van een open en kritische cultuur waarin men van elkaar leert en elkaar als professionals aanspreekt op de gezamenlijke verantwoordelijkheid van gegevensbescherming.

Operationeel niveau

Medewerkers moeten zich bewust zijn van hun rol in het beschermen van persoonsgegevens en ze moeten weten hoe ze dit in de praktijk kunnen vormgeven. Specifieke aandacht moet hierbij uitgaan naar veilige manieren om gegevens te verwerken. Organisatorische maatregelen moeten hieraan ondersteunend zijn, bijvoorbeeld door risicovolle situaties in het proces op te lossen. Een concreet voorbeeld: in plaats van een klant of dienstverlener allerlei persoonsgegevens via de mail toe te sturen, moet worden nagedacht of de klant/dienstverlener de gegevens rechtstreeks kan raadplegen via zijn 'mijnstadsbank'-autorisatie.
Bij het borgen van gegevensbescherming is de mens, in dit geval de medewerker, de zwakste schakel. Bewustwording (awareness) creëren en vasthouden is het belangrijkste middel om van de zwakste schakel de sterkste schakel te maken.

Bewustwording vasthouden

Alle aandacht voor de AVG in de media maakt het voorafgaand aan de invoering relatief eenvoudig om bewustwording over gegevensbescherming te realiseren. Het wordt de uitdaging om die bewustwording vast te houden na de implementatiefase. Het beschermen van persoonsgegevens is tenslotte een continu proces.
De bewaking hiervan vindt plaats door de toetsing van de beveiligingsmaatregelen door de CISO en de jaarlijkse rapportage hierover. Aanvullend rapporteert de FG in deze jaarlijkse rapportage over voortgang en stand van zaken rond de gegevensbescherming. Daarnaast worden instrumenten als het periodiek inzetten van een mystery guest of ethisch hacker ingezet om het bewustzijn van medewerkers te toetsen en ervoor te zorgen dat de tijdens de implementatiefase van de BIG en AVG verkregen bewustwording wordt vastgehouden.

6. Voorzieningen voor betrokkenen

De Stadsbank heeft als verwerkingsverantwoordelijke een informatieplicht op basis van het eerdergenoemde transparantiebeginsel. Aan deze informatieplicht wordt voldaan met het publiceren van het privacy-statement op de website. In deze verklaring worden betrokkenen geattendeerd op de rechten, die zij in het kader van gegevensbescherming hebben en op welke wijze zij in deze rechten kunnen voorzien. Een deel van deze rechten bestaat ook al onder de huidige Wet bescherming persoonsgegevens (met name het recht op inzage, correctie en het indienen van een klacht). De AVG kent daarnaast een aantal nieuwe rechten waarop een betrokkene een beroep kan doen.

Gegevenswissing

Nieuw is het recht op gegevenswissing, dat ook wel het recht op 'vergetelheid' wordt genoemd. We zijn verplicht de gegevens van betrokkene zo snel mogelijk te wissen als:

- Persoonsgegevens niet langer nodig zijn voor de doeleinden waarvoor zij zijn verzameld;
- De verwerking plaatsvindt op basis van toestemming van betrokkene en deze toestemming wordt ingetrokken (NB: over het algemeen zal een gegevensverwerking binnen de Stadsbank eerder plaatsvinden op basis van een overeenkomst of een wettelijke plicht);
- Betrokkene bezwaar maakt tegen de verwerking;
- De persoonsgegevens onrechtmatig verwerkt zijn.

De proceseigenaren moeten onderzoeken of er mogelijk aanpassingen in procedures, programmatuur of software noodzakelijk zijn om aan dit recht gevolg te kunnen geven.

Overdraagbaarheid van gegevens

Ook het recht op overdraagbaarheid van gegevens ('dataportabiliteit') is nieuw. Dat houdt in dat betrokkenen op een makkelijke manier een digitale kopie van hun opgeslagen persoonsgegevens moeten kunnen opvragen. Dit gaat alleen maar om de gegevens die door de betrokkene zelf zijn verstrekt, en dus niet om een volledig dossier. Voorwaarde voor dit recht is dat de verwerking berust op toestemming van betrokkene of noodzakelijk is voor de uitvoering van een overeenkomst. De betrokkene heeft dan het recht om door hem verstrekte persoonsgegevens op te vragen, in een gestructureerde, gangbare en digitale vorm. Dit kan bijvoorbeeld gaan spelen wanneer iemand wil overstappen naar een andere organisatie voor schuldhulpverlening. Als dat door betrokkene gewenst wordt en het is technisch haalbaar, moeten de gegevens rechtstreeks worden doorgezonden naar de andere organisatie.

Beperken verwerking

Nieuw is ook het recht van een betrokkene onder omstandigheden de verwerking van persoonsgegevens te beperken. Dat kan het geval zijn als hij bijvoorbeeld twijfelt over de juistheid van de gegevens. Het recht op beperking betekent dat de persoonsgegevens (tijdelijk) alleen verwerkt mogen worden met toestemming van de betrokkene. Dit geldt alleen niet voor de opslag van de gegevens. Aandachtspunt voor de praktijk hierbij is dat bij de betreffende persoonsgegevens duidelijk moet worden aangegeven dat de verwerking van de persoonsgegevens beperkt is. Medewerkers moeten dus weten wanneer dit recht wordt uitgeoefend zodat de betreffende gegevens bijvoorbeeld niet

worden gedeeld. Ook hiervoor zullen mogelijk aanpassingen in de software of in werkprocessen moeten worden aangebracht. Als de beperking weer wordt opgeheven, moet de betrokkene hiervan op de hoogte worden gebracht.

Bezwaar

Een betrokkene kan op basis van zijn specifieke situatie en onder voorwaarden bezwaar maken tegen de verwerking van zijn persoonsgegevens. Dit is overigens niet een bezwaar als bedoeld in de Algemene wet bestuursrecht. Als een betrokkene bezwaar maakt, dan moet de verwerking in principe worden gestaakt, tenzij er dwingende gerechtvaardigde gronden zijn die zwaarder wegen dan het belang van de betrokkene. Een voorbeeld daarvan is bijvoorbeeld een wettelijke verplichting.

Geautomatiseerde individuele besluitvorming / profilering

Verder heeft een betrokkene het recht om niet te worden onderworpen aan geautomatiseerde individuele besluitvorming, waaronder profilering. Bij dit recht kan bijvoorbeeld gedacht worden aan de automatische weigering van een online ingediende kredietaanvraag of aan de verwerking van sollicitaties via internet zonder menselijke tussenkomst.

De FG houdt namens de Autoriteit Persoonsgegevens toezicht op de naleving van deze rechten van betrokkenen. Hij bekleedt hierin een onafhankelijke positie. Dat betekent dat een aanwijzing om invulling te geven aan deze rechten niet door een proceseigenaar opzij kunnen worden geschoven. Het gaat hierbij namelijk om in de AVG vastgelegde rechten en niet om beveiligingsmaatregelen.

Laagdrempelige uitoefening

Over de verwerking van persoonsgegevens moet helder worden gecommuniceerd. Alle rechten van betrokkenen moeten worden vertaald in laagdrempelige procedures. In het privacy-statement is aangegeven op welke wijze meldingen, bezwaar en klachten over de gegevensverwerking kunnen worden gemeld. Hiervoor wordt verwezen naar de contactgegevens van de Functionaris Gegevensbescherming.

Als een betrokkene gebruik maakt van zijn rechten, moet er zo snel mogelijk, maar uiterlijk binnen één maand na ontvangst van het verzoek informatie worden gegeven over wat er met het verzoek is gedaan. Deze termijn kan bij omvangrijke of ingewikkelde verzoeken met nog eens twee maanden worden verlengd.

Borging gegevensbescherming

Blijvende bewustwording bij het beschermen van persoonsgegevens op alle niveaus in de organisatie is essentieel. Technische ontwikkelingen, voortschrijdende inzichten, wijzigingen in wet- en regelgeving en 'best practices' kunnen aanpassingen in het beleid en/of de uitvoering noodzakelijk maken. Daarom wordt de werking van de gegevensbescherming in de praktijk regelmatig (in ieder geval jaarlijks) geëvalueerd door de CISO, met input van de FG.

Om aantoonbaar te maken dat de AVG wordt nageleefd, fungeert het ISMS tevens als dossier voor gegevensbescherming. Alle relevante documenten worden hierin gekoppeld

aan de van toepassing zijnde beveiligingsmaatregelen en overzichtelijk bij elkaar bewaard, zoals het register van verwerkingsactiviteiten, rapporten van PIA's, audits en dergelijke. Het ISMS vormt een belangrijk instrument om aan te tonen dat de Stadsbank zowel aan de afspraken in het kader van informatiebeveiliging als aan de voorschriften omtrent privacy voldoet.

7. De beveiligingsmaatregelen

De inrichting van de maatregelen op het gebied van informatiebeveiliging is gebaseerd op de Baseline Informatiebeveiliging Gemeenten (BIG). De BIG is een vertaling van de ISO 27001-norm. Deze internationale norm is van toepassing op alle typen organisaties (bijvoorbeeld commerciële ondernemingen, overheidsinstanties, non-profitorganisaties). De norm specificeert eisen voor het vaststellen, implementeren, uitvoeren, controleren, beoordelen, bijhouden en verbeteren van een gedocumenteerd Information Security Management System (ISMS) in het kader van de algemene bedrijfsrisico's voor de organisatie.

De norm specificeert eisen voor de implementatie van beveiligingsmaatregelen die zijn aangepast aan de behoeften van afzonderlijke organisaties of delen daarvan. Op basis van deze behoeften moet de keuze van adequate en proportionele beveiligingsmaatregelen worden gemaakt die de informatie beschermen en vertrouwen bieden aan belanghebbenden. ISO27001 en de hierop gebaseerde BIG onderscheiden een aantal beveiligingsdomeinen. Deze domeinen worden hieronder toegelicht. De beveiligingsmaatregelen worden nader uitgewerkt en bewaakt in het ISMS.

Uitwerking van het beleid in het beveiligingsplan

Aan alle beveiligingsmaatregelen die in de BIG genoemd staan is een actiehouder gekoppeld. Hieronder is aangegeven wie op de verschillende domeinen van de BIG als actiehouder wordt aangewezen. Per onderliggende maatregel kan een andere actiehouder zijn aangewezen.

NB: de verantwoordelijkheid voor het treffen van beveiligingsmaatregelen ligt te allen tijde bij de lijnmanager, die eigenaar is van het te beveiligen proces. De actiehouder fungeert tijdens de implementatie van de maatregelen als aanspreekpunt voor de lijnmanager en zorgt dat duidelijk is welke maatregelen getroffen moeten worden. In onderstaande tabel is per beveiligingsdomein aangegeven wie de actiehouder is. Uiteindelijk beslist de lijnmanager of de voorgestelde beveiligingsmaatregelen worden toegepast. Als een maatregel niet wordt getroffen, moet duidelijk zijn waarom van de maatregel wordt afgezien. De uitleg voor het achterwege laten van de maatregel wordt vastgelegd in het ISMS.

Acceptatie door de manager

Er kan op verschillende manieren met (rest) risico's worden omgegaan. De meest gebruikelijke strategieën zijn:

<u>Risicodragend</u>

Risicodragend wil zeggen dat risico's geaccepteerd worden. Dat kan zijn omdat de kosten van de beveiligingsmaatregelen de mogelijke schade overstijgen. Maar het management kan ook besluiten om niets te doen, ondanks dat de kosten niet hoger zijn dan de schade die kan optreden.

Risiconeutraal

Onder risiconeutraal wordt verstaan dat er dusdanige beveiligingsmaatregelen worden genomen dat dreigingen óf niet meer manifest worden óf, wanneer de dreiging wel manifest wordt, de schade als gevolg hiervan geminimaliseerd is.

Risicomijdend

Onder risicomijdend verstaan we dat er zodanige maatregelen worden genomen dat de dreigingen zo veel mogelijk worden geneutraliseerd, zodat de dreiging niet meer tot een incident leidt. Denk hierbij aan het invoeren van nieuwe software waardoor de fouten in de oude software geen dreiging meer vormen. In simpele bewoordingen: een ijzeren emmer kan roesten. Neem een kunststof emmer en de dreiging, roest, valt weg.
Welke strategie een organisatie ook kiest, de keuze dient bewust door het management te worden gemaakt en de gevolgen ervan dienen te worden gedragen.

Het geheel van getroffen en niet getroffen maatregelen wordt ter goedkeuring voorgelegd aan het Dagelijks Bestuur. De CISO ziet vervolgens jaarlijks toe op de naleving van de afspraken en rapporteert hierover aan het Dagelijks Bestuur in de P&C cyclus.

Beveiligingsdomeinen en ISMS-systeem

In onderstaande tabel zijn de tien verschillende beveiligingsdomeinen van de BIG[1] aangegeven en is een actiehouder benoemd. Het ISMS-systeem is conform deze indeling ingericht. De beveiligingsdomeinen worden hierna toegelicht.

BIG-domein	Actiehouder
5. Informatiebeveiligingsbeleid	
6. Organisatie van de informatiebeveiliging	Manager Bedrijfsvoering en Advies
7. Beheer van bedrijfsmiddelen	Security Officer (SO)
8. Personele beveiliging	Personeelsfunctionaris
9. Fysieke beveiliging en beveiliging van de omgeving	Adviseur facilitaire dienstverlening
10. Beheer van communicatie- en bedieningsprocessen	Functioneel applicatiebeheerder
10. Logische toegangsbeveiliging	Functioneel applicatiebeheerder
11. Verwerving, ontwikkeling en onderhoud van informatiesystemen	Manager Bedrijfsvoering en Advies
12. Beheer van beveiligingsincidenten	Security Officer (SO)
13. Bedrijfscontinuïteitsbeheer	Manager Bedrijfsvoering en Advies
Naleving	CISO

[1] De BIG kent vier inleidende hoofdstukken en nummert de bovenstaande domeinen van 5 t/m 1.

Domein 1/5: Informatiebeveiligingsbeleid

Doelstelling van de maatregelen in dit domein is het borgen van betrouwbare dienstverlening en een aantoonbaar niveau van informatiebeveiliging dat voldoet aan de relevante wetgeving, algemeen wordt geaccepteerd door haar (keten-)partners en er mede voor zorgt dat de kritische bedrijfsprocessen bij een calamiteit en incident voortgezet kunnen worden. De volgende maatregelen hebben betrekking op dit domein:

- Informatiebeveiligingsbeleid behoort door het hoogste management te worden goedgekeurd en gepubliceerd. Het document dient tevens kenbaar te worden gemaakt aan alle werknemers en relevante externe partijen.

Aan deze maatregel wordt invulling gegeven door het informatiebeveiligingsbeleid door het Dagelijks Bestuur te laten vaststellen.

- Het informatiebeveiligingsbeleid behoort met geplande tussenpozen, of zodra zich belangrijke wijzigingen voordoen, te worden beoordeeld om te bewerkstelligen dat het geschikt, toereikend en doeltreffend blijft.

Door de aanwijzing van de Chief Information Security Officer (CISO) en deze toe te laten zien op het geheel van beveiligingsmaatregelen wordt aan deze maatregel voldaan.

Domein 2/6: Organisatie van de beveiliging

Voor de organisatie van de beveiliging is een governance-structuur ingericht. Deze structuur is beschreven in het onderdeel beveiligingsorganisatie van het informatiebeveiligingsbeleid. Doelstelling van deze structuur is het beheren en waarborgen van informatiebeveiliging en gegevensbescherming binnen de organisatie van de Stadsbank en haar verwerkers. De volgende maatregelen hebben betrekking op dit domein:

- Het hoogste management behoort actief informatiebeveiliging binnen de organisatie te ondersteunen door duidelijk richting te geven, betrokkenheid te tonen en expliciet verantwoordelijkheden voor informatiebeveiliging toe te kennen en te erkennen.

Aan deze maatregel wordt invulling gegeven door het informatiebeveiligingsbeleid door het Dagelijks Bestuur te laten vaststellen.

- Activiteiten voor informatiebeveiliging behoren te worden gecoördineerd door vertegenwoordigers uit de verschillende delen van de organisatie met relevante rollen en functies.
- Alle verantwoordelijkheden voor informatiebeveiliging behoren duidelijk te zijn gedefinieerd.

Aan deze maatregelen wordt invulling gegeven door de vaststelling door het Dagelijks Bestuur van de in het beleid voorgestelde beveiligingsorganisatie.

Overige maatregelen binnen dit domein worden in het ISMS verder uitgewerkt en voorzien van een actiehouder:

Domein 3/7: Beheer van bedrijfsmiddelen

Het gaat in dit beveiligingsdomein om het beheer en het vaststellen van de benodigde beveiliging van ICT-middelen zoals servers, laptops, werkstations, mobiele apparaten, usb-sticks, maar ook sleutels of toegangspasjes en dergelijke. In het ISMS wordt

beschreven welke beheermaatregelen worden genomen om deze bedrijfsmiddelen te beschermen. Deze maatregelen bestaan onder andere uit:

- Het bijhouden van een inventarislijst van alle apparaten en een hieraan toegewezen eigenaar. Deze inventarisatie vindt plaats in TopDesk.
- Een uitgifte- en innameprocedure voor bedrijfsmiddelen (procedure wijzigings- en configuratiebeheer).
- Regels voor het gebruik van de bedrijfsmiddelen, zoals geen laptops mee naar huis zonder toestemming, geen illegale software installeren, wel of geen privégebruik toestaan e.d. Deze regels worden vastgelegd in de huisregels en gedragscode voor medewerkers.
- Gegevensclassificatie. Hierbij worden de gegevensstromen in de organisatie van de Stadsbank ingedeeld aan de hand van het benodigde niveau van beschikbaarheid, integriteit en vertrouwelijkheid. Op basis hiervan wordt het passende niveau van informatiebeveiliging bepaald. Uitgangspunt is dat de Stadsbank gebruik maakt van gegevens met een vertrouwelijk karakter, waarbij een hoog niveau van beveiliging past.

Domein 4/8: Beveiligingsmaatregelen t.a.v. personeel

In dit domein gaat het om maatregelen die ervoor zorgen dat medewerkers, ingehuurd personeel en eventuele externe gebruikers weten welke verantwoordelijkheden ze hebben bij de informatiebeveiliging. Het doel is om zo het risico van diefstal, fraude of misbruik van informatie te verminderen. Maatregelen binnen dit beveiligingsdomein, die in het ISMS verder worden uitgewerkt, zijn onder andere de volgende:

- Maatregelen bij indiensttreding van het personeel, bijvoorbeeld het ondertekenen van geheimhoudingsverklaringen en het overleggen van een VOG en eventuele screening van kandidaten.
- Een procedure die duidelijk maakt wie bepaalt welke rol(len) medewerkers vervullen en welke autorisatie voor gebruik van persoonsgegevens wordt verstrekt.
- Maatregelen bij tussentijdse verandering van functies om bijvoorbeeld opeenstapeling van bevoegdheden te voorkomen.
- Maatregelen in het kader van bewustwording, bijvoorbeeld periodieke aandacht voor informatieveiligheid in werkoverleggen of via trainingen. Deze maatregelen worden vastgelegd in een communicatieplan.

Domein 5/9: Fysieke beveiliging

In dit onderdeel van het ISMS wordt vastgelegd hoe de organisatie wordt beschermd tegen fysieke bedreigingen en gevaren van buitenaf. Het gaat er bijvoorbeeld om te voorkomen dat onbevoegden toegang krijgen tot het gebouw, tot (fysieke) informatie en bedrijfsmiddelen. Maatregelen zijn onder andere:

- Maatregelen om schade door brand, overstroming, explosies, oproer, stroomonderbreking e.d. te beperken (bijvoorbeeld door verzekeringen).
- Fysieke toegangsbeveiliging (druppel, camera's).
- ICT-voorzieningen, die kritieke of gevoelige bedrijfsactiviteiten ondersteunen, staan in een afgeschermde beveiligde ruimte.
- Een overzicht wie toegang hebben tot ruimten waar zich informatie- en ICT-voorzieningen bevinden en een registratie van verleende toegang.
- Reserveapparatuur en back-ups staan op een andere locatie om de gevolgen van een calamiteit te beperken.

- Procedures rond het verwijderen of overschrijven van gegevens en programmatuur voordat apparaten worden afgevoerd.

Domein 6/10: Beheer van communicatie en bedieningsprocessen

Doelstelling van de maatregelen in dit domein is het waarborgen van een correcte en veilige bediening van ICT-voorzieningen. Hierbij kan worden gedacht aan de volgende maatregelen:

- Bedieningsprocedures behoren te worden gedocumenteerd, te worden bijgehouden en beschikbaar te worden gesteld aan alle gebruikers die deze nodig hebben.
- Wijzigingsbeheer (wijzigingen in ICT-voorzieningen en informatiesystemen behoren te worden beheerst).
- Functiescheiding (Taken en verantwoordelijkheidsgebieden behoren te worden gescheiden om gelegenheid voor onbevoegde of onbedoelde wijziging of misbruik van de bedrijfsmiddelen van de organisatie te verminderen).
- Bescherming tegen virussen.
- Het maken van back-ups om de integriteit en beschikbaarheid van informatie en ICT-voorzieningen te handhaven.
- Enz.

Domein 7/11: Toegangsbeveiliging

Doelstelling van de maatregelen in dit domein is het beheersen van de toegang tot informatie, door middel van:

- Het vaststellen van toegangsbeleid op basis van organisatie-eisen en beveiligingseisen voor toegang.
- Het bewerkstelligen van toegang voor bevoegde gebruikers bewerkstelligen en het voorkomen van onbevoegde toegang tot informatiesystemen.
- Enz.

Domein 8/12: Verwerving, ontwikkeling en onderhoud van informatiesystemen

Doelstelling van de maatregelen in dit domein is te bewerkstelligen dat informatiebeveiliging integraal deel uitmaakt van informatiesystemen. Dit gebeurt onder andere door het toepassen van 'privacy by design' voorafgaand aan de aanschaf van nieuwe informatiesystemen, en 'privacy by default' bij het in gebruik nemen van een nieuw of gewijzigd informatiesysteem.

Domein 9/13: Beheer van beveiligingsincidenten

Doelstelling van de maatregelen in dit domein is het bewerkstelligen dat informatiebeveiligings-gebeurtenissen en zwakheden die verband houden met informatiesystemen zodanig kenbaar worden gemaakt dat tijdig corrigerende maatregelen kunnen worden genomen.

Domein 10/14: Bedrijfscontinuïteitsbeheer

Doelstelling van de maatregelen in dit domein is het tegengaan van onderbreking van bedrijfsactiviteiten en bescherming van kritische bedrijfsprocessen tegen de gevolgen van omvangrijke storingen in informatiesystemen of rampen en om tijdig herstel te bewerkstelligen. Hiervoor worden onder andere de volgende maatregelen getroffen:

- Er behoort een beheerd proces voor bedrijfscontinuïteit in de gehele organisatie te worden ontwikkeld en bijgehouden, voor de naleving van eisen voor informatiebeveiliging die nodig zijn voor de continuïteit van de bedrijfsvoering.

- Het uitvoeren van een Business Impact Analyse (BIA) om de risico's te identificeren die kunnen leiden tot verstoring van het bedrijfsproces.
- Er behoren plannen te worden ontwikkeld en geïmplementeerd om de bedrijfsactiviteiten te handhaven of te herstellen en om de beschikbaarheid van informatie op het vooraf afgesproken niveau en binnen in de vereiste tijdspanne te bewerkstelligen na onderbreking of uitval van kritische bedrijfsprocessen.

Domein 11/15: Naleving

Doelstelling van deze maatregel is het voorkomen van schending van enige wetgeving, wettelijke en regelgevende of contractuele verplichtingen, en van beveiligingseisen en te bewerkstelligen dat systemen voldoen aan het beveiligingsbeleid en de beveiligingsnormen van de organisatie. De CISO en FG zien toe op de naleving van de beveiligingsmaatregelen in de organisatie.

8. Begrippenlijst (Alfabetisch)

Accountability / verantwoordingsplicht

Een persoon of organisatie die verantwoordelijk is voor een verwerking toont aan dat er maatregelen zijn genomen om aan de AVG te voldoen en privacyrisico's uit te bannen of te beperken. Hieronder valt ook het toetsen of de maatregelen in de praktijk voldoende zijn.

AVG (GDPR)

De Algemene Verordening Gegevensbescherming. Dit is de Nederlandse vertaling van de General Data Protection Regulation, welke door de Europese lidstaten per 25 mei 2016 is ingesteld. De AVG treedt twee jaar na deze vaststelling in werking, dus per 25 mei 2018. Met de inwerkingtreding van de AVG vervalt de Wet bescherming persoonsgegevens (Wbp)

Baseline Informatiebeveiliging Gemeenten (BIG)

Dit is een beveiligingsstandaard voor overheidsinstanties. Deze standaard is ontwikkeld door de Informatie Beveiligings Dienst (IBD), een samenwerkingsverband van de Vereniging van Nederlandse Gemeenten (VNG) en het Kwaliteitsinstituut Nederlandse Gemeenten (KING). De BIG is algemeen aanvaard als de norm voor informatiebeveiliging binnen gemeenten. Op termijn wordt de BIG vervangen door de Baseline Informatiebeveiliging Overheid, waarmee de normstelling voor rijk, gemeenten en waterschappen op het gebied van informatiebeveiliging wordt geharmoniseerd.

Betrokkene

Degene van wie persoonsgegevens worden verwerkt.

Dataportabiliteit / overdraagbaarheid van gegevens

Dit is het recht van personen om op een makkelijke manier een elektronische kopie van door hem / haar zelf verstrekte persoonsgegevens op te vragen. Voorwaarde hierbij is dat de verwerking berust op toestemming van de betrokkene of noodzakelijk is voor de uitvoering van een overeenkomst.

Encryptie

Het versleutelen van gegevens, waardoor de gegevens onleesbaar zijn als je niet over de beveiligingssleutel beschikt. Dit is een beveiligingsmaatregel die voorkomt dat gegevens kunnen worden ingezien als ze door onbevoegden worden onderschept.

Logging

Het verzamelen van gegevens over een proces of systeem. Een log beschrijft wat er is gebeurd binnen een systeem. Logging kan gebruikt worden om informatie op te slaan

over wie toegang heeft tot een systeem of data, over fouten of over andere gebeurtenissen die aandacht behoeven van de gebruiker of beheerder.

Persoonsgegeven

Een persoonsgegeven is elk gegeven over een geïdentificeerde of identificeerbare natuurlijke persoon. Dit betekent dat informatie ofwel direct over iemand gaat, ofwel naar deze persoon te herleiden is. Het gaat erom of iemand kan worden onderscheiden van anderen (kan worden herkend in een groep). Gegevens van organisaties of van overleden personen zijn geen persoonsgegevens.

Privacy by Design en Privacy by Default

Privacy by Design houdt in dat in een nieuwe werkwijze al bij het ontwerp ervan rekening wordt gehouden met de bescherming van persoonsgegevens. In het ontwerp wordt voor de minst privacy- belastende werkwijze gekozen waarbij de minste data wordt verwerkt.

Privacy by Default betekent dat je je standaardinstellingen op 'uit' zet en dat iemand zelf kan kiezen om deze aan te zetten, bijvoorbeeld een vinkje om gegevens te delen.

Privacyeffectbeoordeling / PIA

Een privacyeffectbeoordeling, ofwel een Privacy Impact Assessment, kortweg PIA, is een uitgebreide vragenlijst. Aan de hand van de antwoorden op de vragen laat de PIA zien hoe groot de kans is dat de privacy van betrokkenen wordt geschaad, waar dit risico zich voordoet en wat de gevolgen daarvan zijn. Met de uitkomsten van een PIA kun je gericht acties ondernemen om de risico's te verminderen of uit te sluiten. De Nederlandse term voor deze PIA is 'gegevensbeschermingseffectbeoordeling'. In de AVG wordt gesproken over DPIA (Data Privacy Impact Assessment).

Profilering

Het verzamelen, analyseren en combineren van (persoons)gegevens met als doel iemand in te delen in een bepaalde categorie. Hiermee kunnen de voorkeuren of het gedrag van een persoon worden geanalyseerd en voorspeld of een beslissing over hem worden genomen. De persoon wordt beoordeeld aan de hand van een (risico)profiel.

Pseudonimisering

Een manier waarbij persoonsgegevens in een aparte dataset worden vervangen door een nummer. Daarmee zijn de gegevens van de nieuwe dataset niet meer herleidbaar tot de persoon. Deze nieuwe dataset en de sleutel tot de oorspronkelijke persoonsgegevens worden apart van elkaar bewaard. Daarnaast zijn er waarborgen om re-identificatie voorkomen (bijv. beleid of contracten). De originele persoonsgegevens zijn echter nog aanwezig, dus is er *geen* sprake van anonieme gegevens (dan zouden de oorspronkelijke data vernietigd zijn of zou re-identificatie onmogelijk zijn gemaakt).

Verwerker

Een verwerker is de persoon of instantie die *ten behoeve van* de verwerkingsverantwoordelijke persoonsgegevens verwerkt. Een verwerker heeft zelf geen doel bij de verwerking en dient de instructies van de verantwoordelijke op te volgen.

Verwerkersovereenkomst

Een verwerkingsverantwoordelijke is verplicht een verwerkersovereenkomst te sluiten als hij een (deel van) zijn verwerkingen uitbesteedt aan een verwerker. Met deze overeenkomst draagt de verwerkingsverantwoordelijke een aantal van zijn wettelijke verplichtingen over op de verwerker. Ondanks deze overeenkomst blijft de verwerkingsverantwoordelijke wel eindverantwoordelijk voor het naleven van de wet- en regelgeving. De AVG stelt een aantal inhoudelijke eisen aan de verwerkersovereenkomst.

Verwerking

Dit zijn alle handelingen die een organisatie kan uitvoeren met persoonsgegevens, al dan niet via een geautomatiseerde manier. Het is een zeer ruim begrip en volgens de AVG gaat het bijvoorbeeld om het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van gegevens.

Verwerkingsverantwoordelijke

Een persoon of instantie is verwerkingsverantwoordelijke als hij alleen, of samen met anderen, het *doel van en de middelen voor* de verwerking vaststelt.

Stadsbank
Oost Nederland

Procedure Configuratiebeheer

Maatregelen BIG die met deze procedure worden onderbouwd

Maatregel 7.1.1	Inventarisatie van bedrijfsmiddelen
Maatregel 7.1.3	Aanvaardbaar gebruik van bedrijfsmiddelen
Maatregel 12.4.1	Beheersing van operationele programmatuur

1.1 Doelstellingen

De Stadsbank hanteert de volgende doelstelling:

- Configuratiebeheer draagt er zorg voor dat de gegevens over de ICT-infrastructuur (ICT-middelen en -diensten) betrouwbaar worden vastgelegd en dat actuele en relevante gegevens aan andere ICT-beheerprocessen worden geleverd over de ICT-middelen, hun onderlinge samenhang (relaties) en de relaties met de ICT-diensten.

De beleidsregels van de Stadsbank met betrekking tot configuratiebeheer zijn:

a) Alle bedrijfsmiddelen moeten geïdentificeerd zijn, er moet een inventaris van worden bijgehouden.
b) Alle informatie en bedrijfsmiddelen die verband houden met ICT-voorzieningen, moeten aan een 'eigenaar' (een deel van de organisatie) zijn toegewezen.
c) Apparatuur, informatie en programmatuur van de organisatie, mogen niet zonder toestemming vooraf, van de locatie worden meegenomen.
d) De verantwoordelijkheid voor specifieke beheersmaatregelen mag door de proceseigenaar worden gedelegeerd, maar de proceseigenaar blijft verantwoordelijk voor een goede bescherming van de bedrijfsmiddelen.
e) Het object van classificatie is informatie. We classificeren op het niveau van informatiesystemen (of informatieservices). Alle classificaties van bedrijfskritische systemen zijn centraal vastgelegd door de Data Protection Officer in het verwerkingsregister, en dienen jaarlijks gecontroleerd te worden door de eigenaren.

1.2 Implementatie

a) Er is een actuele registratie van bedrijfsmiddelen die voor de organisatie een belang vertegenwoordigen zoals informatie(verzamelingen), software, hardware, diensten, mensen en hun kennis/vaardigheden.
b) Van elk middel is het vereiste beschermingsniveau en de verantwoordelijke lijnmanager bekend.

1.3 Bekendmaking

De inhoud van deze procedure moet bekend zijn bij alle medewerkers die bij de inventarisatie, inrichting en toewijzing van bedrijfsmiddelen betrokken zijn.

1.4 Aanleiding

Configuratiebeheer is voorwaardenscheppend voor bijna alle andere ICT-beheerprocessen. Configuratiebeheer is van belang in het kader van de integriteitshandhaving, doordat het proces borgt dat updates van configuratie-items overal worden aangebracht waar ze worden gebruikt. Daarnaast legt het proces Configuratiebeheer de beveiligingsclassificatie van alle configuratie-items vast. Deze classificatie kan worden gebruikt om beveiligingsmaatregelen beter toe te snijden op de risico's van het hebben of gebruiken van configuratie-items, al dan niet afhankelijk van de soort omgeving of het type bedrijfsproces.

1.5 Definities

De gegevens over de ICT-infrastructuur (ICT-middelen en -diensten) worden aangeduid als configuratie-items (= CI) en hebben betrekking op hard- en software, netwerkverbindingen en documentatie en worden in een geautomatiseerde database, de Configuratie Management Database (CMDB), vastgelegd. Tevens wordt de onderlinge samenhang tussen deze componenten vastgelegd. De informatiebehoeften van afhankelijke ICT-beheerprocessen bepalen de aard en diepgang van de vastleggingen over configuratie-items.

1.6 Proceseigenaar

De proceseigenaar is de lijnmanager onder wiens verantwoordelijkheid het gebruik van bedrijfsmiddelen of de hierin vastgelegde informatie valt. Voor het proces Configuratiebeheer is dit de manager Bedrijfsvoering en Advies. Uitvoering van dit proces ligt in handen van de SO.

1.7 Verantwoordelijkheid

De verantwoordelijkheid voor deze procedure ligt te allen tijde bij het Dagelijks Bestuur en namens deze bij de manager Bedrijfsvoering en Advies.

1.8 Actualiteit

De manager Bedrijfsvoering en Advies is verantwoordelijk voor het actueel houden van deze procedure. Indien de procedure inhoudelijk wijzigt, draagt de SO zorg voor communicatie daarover en distributie en archivering van de procedure.

1.9 Uitvoering

Deze procedure is van toepassing op de gehele IT-infrastructuur, voor zover deze niet is uitbesteed aan ROOT, en is geldig vanaf het moment van levering van goederen, of identificatie van bestaande nog niet geregistreerde CI's, tot het moment dat de CI's geregistreerd zijn en er een melding van configuratiebeheer is uitgegaan dat het CI in productie kan worden genomen. Het beheer van infrastructuur-componenten door ROOT wordt vastgelegd in de verwerkersovereenkomst.

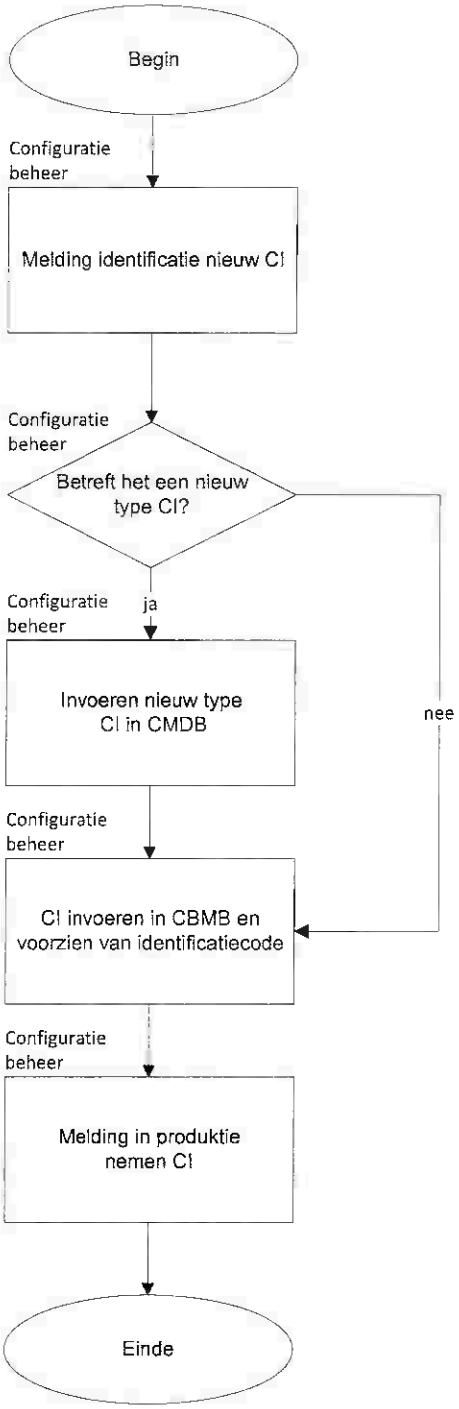
De hoofdactiviteiten van dit proces zijn als volgt:

- Identificatie van configuratie items
- Beheer van de configuratiebeheer database (CMDB)

- Statusbewaking van de configuratie items
- Verificatie van de CMDB.

Identificatie van configuratie items

In onderstaand stroomschema wordt deze hoofd activiteit in beeld gebracht:



1.
Configuratiebeheer krijgt van verschillende kanten meldingen van nieuwe CI's.

- Wijzigingsbeheer. Nadat de adviseur Facilitaire Dienstverlening een levering van goederen gecontroleerd heeft op juistheid en volledigheid registreert hij/zij de CI-gegevens van deze goederen.
- Als er tijdens de dagelijkse werkzaamheden een CI gesignaleerd wordt dat nog niet in de CMDB staat ,wordt dit gemeld aan configuratiebeheer.

2.
Indien het CI van een type (artikel) is, dat nog niet eerder is ingezet en waarvan het type nog niet in de CMDB staat, dan moet beslist worden of het nieuwe type CI in de CMDB ingevoerd wordt. In het geval van een levering bestaat het type CI al, omdat bij een goedgekeurde bestelling het type CI al in de CMDB is geregistreerd.
Zo ja, ga naar stap 3. Zo nee, ga naar stap 4.

3.
Indien er sprake is van signalering van een nieuw type CI, dat al ingezet is, gaat de SO bij de betreffende lijnmanager na of dit nieuwe type geautoriseerd is volgens afspraken. Mogen CI's van dit type volgens de vastgestelde lijst met standaarden worden ingezet, of wordt de lijst indien nodig aangepast? Indien dit is toegestaan wordt er een nieuw type in de CMDB aangemaakt.

4.

Het CI wordt door de SO voorzien van een label waarop een unieke identificatiecode staat. De CI gegevens worden in de CMDB ingevoerd. Hierna wordt het CI gekoppeld aan het bijbehorende type in de CMDB. Indien het CI relaties heeft met andere CI's worden deze koppelingen vastgelegd.

5.
In het geval van levering van gebruikersgoederen (printers en dergelijke) geeft de SO door, dat de aangevraagde CI's ingevoerd zijn. Het CI kan in productie worden genomen en geïnstalleerd bij de gebruiker.
Voor overige goederen geldt dat de betrokken specialisten door de lijnmanager op de hoogte worden gesteld.

<u>Beheer van de configuratiebeheer database (CMDB)</u>

6.
Wijzigingen op CI's kunnen door verschillende functionarissen en als gevolg van verschillende oorzaken aan Configuratiebeheer gemeld worden, bijvoorbeeld:

- Functioneel beheer is een incident aan het oplossen en constateert een fout in de CMDB.
- De adviseur Facilitaire Dienstverlening ontvangt nieuwe hard- en/of software.
- Een leverancier heeft wijzigingen doorgevoerd.

De wijziging moet goedgekeurd zijn door het proces Wijzigingsbeheer. In het geval van standaardwijzigingen kan van goedkeuring worden uitgegaan. De uitvoerder van een wijziging controleert of er mogelijk ook andere CI's wijzigen als gevolg van een door hem gemaakte aanpassing in de IT-infrastructuur.

7.
Indien er als gevolg van de wijziging een CI van een type (artikel) ontstaat, wat nog niet eerder is ingezet en waarvan het type nog niet in de CMDB staat, dan moet eerst het nieuwe type CI in de CMDB ingevoerd worden.

Zo ja, ga naar stap 8. Zo nee, ga naar stap 9.

8.
Configuratiebeheer gaat bij de manager Bedrijfsvoering en Advies na of dit nieuwe type geautoriseerd is volgens afspraken. Mogen CI's van dit type volgens de vastgestelde lijst standaard worden ingezet? Indien dit is toegestaan wordt er een nieuw type in de CMDB aangemaakt.

9.
Configuratiebeheer verifieert of de wijziging goedgekeurd is door wijzigingsbeheer. De CI's worden in de CMDB aangepast aan de hand van de via de aanmelder ontvangen gegevens, zodat de CMDB weer overeenkomt met de fysieke situatie van de CI's. Als gevolg van de wijziging kan het mogelijk zijn dat de status van een CI in de CMDB moet worden veranderd.

10.
Wijziging op een CI kan de gegevens van andere CI's, of de koppeling met andere CI's veranderen. Dit moet door de melder doorgegeven worden. Omdat dit vaak moeilijk door de aanmelder te bepalen is controleert de SO ook zelf a.d.h.v. de CMDB of er nog andere koppelingen of CI's moeten worden aangepast. De SO voert deze wijzigingen in de CMDB door onder vermelding van de wijzigingsdatum.

11.
De SO geeft aan de aanmelder door dat de wijziging in de CMDB is doorgevoerd. Tevens deelt de SO mee of er andere CI's of koppelingen zijn aangepast.

Statusbewaking van de configuratie items

12.
De in de CMDB geregistreerde gegevens worden vergeleken met de werkelijkheid.

- Tijdens de dagelijkse werkzaamheden kunnen door de functioneel beheerders afwijkingen worden geconstateerd
- De functioneel beheerders zijn in een afgebakende periode bezig met een geplande verificatieslag waarin een groot aantal CI's worden gecontroleerd. Configuratiebeheer coördineert dit.

13.
Als geconstateerd wordt dat de geregistreerde gegevens afwijken van de werkelijke situatie, ga dan naar stap 14. Zo nee, ga naar stap 15.
Als de geplande verificatie beëindigd is (alle te verifiëren CI's zijn vergeleken), ga dan naar stap 14. Zo nee, ga naar stap 15.

14.
De geconstateerde afwijking wordt doorgegeven aan Configuratiebeheer.

Verificatie van CMDB

15.
De SO analyseert de afwijking om te achterhalen wat de oorzaak is. Als de oorzaak bekend is kunnen maatregelen worden genomen om herhaling van een afwijking te voorkomen.

16.
De wijziging wordt doorgevoerd.

17.
Als het een continue afwijking betrof, ga dan naar stap 6.
Als de geplande verificatieslag nog niet is afgerond, ga dan naar stap 9.
Zo nee, ga naar stap 1.

18.
Configuratiebeheer rapporteert aan de manager Bedrijfsvoering en Advies over de afwijkingen die de geplande verificatie heeft opgeleverd.

Beheersmaatregel:	7.1.1
Documentversie:	1.0
Documentnaam:	7.1.1 Procedure Configuratiebeheer.docx

Stadsbank
Oost Nederland

Voorstel

Aan: Dagelijks Bestuur

Van: Directeur

Datum: 5 juli 2018

Betreft: Notitie 'Verklaring van Toepasselijkheid'

Te besluiten:

1. In te stemmen met de notitie 'Verklaring van Toepasselijkheid' in het kader van het informatiebeveiligingsbeleid van de Stadsbank Oost Nederland.

Toelichting:

Het doel van de notitie 'Verklaring van Toepasselijkheid' is om verantwoording af te leggen over de implementatie van maatregelen uit de Baseline Informatiebeveiliging Gemeenten (BIG), die passend zijn voor de Stadsbank Oost Nederland, als ook om restrisico's goed te keuren en formele goedkeuring te verkrijgen voor de implementatie van de passende maatregelen.

Uitgangspunten voor deze 'Verklaring van Toepasselijkheid':

- De Baseline Informatiebeveiliging Gemeenten (BIG) is de leidraad voor de inrichting van een systeem van beveiligingsmaatregelen, dat waarborgen biedt voor de beschikbaarheid, integriteit, vertrouwelijkheid en controleerbaarheid van de door de Stadsbank gebruikte informatiesystemen.
- De keuze voor de te implementeren maatregelen is gerelateerd aan de praktische toepasbaarheid van deze maatregelen in de omgeving van de Stadsbank Oost Nederland.

Deze notitie bevat de planning van alle beheermaatregelen vermeld in de BIG, voor zover van toepassing verklaard door het Information Security Team en het MT van de Stadsbank. Deze beheermaatregelen zijn vastgelegd in het Information Security Management System (ISMS), dat wordt beheerd door de Chief Information Security Officer (CISO).

De beveiligingsrisico's die worden geaccepteerd staan expliciet vermeld in paragraaf 4 van de notitie. De beheermaatregelen die zijn opgenomen in de BIG om deze risico's te verminderen of weg te nemen zullen niet door de Stadsbank worden geïmplementeerd omdat :

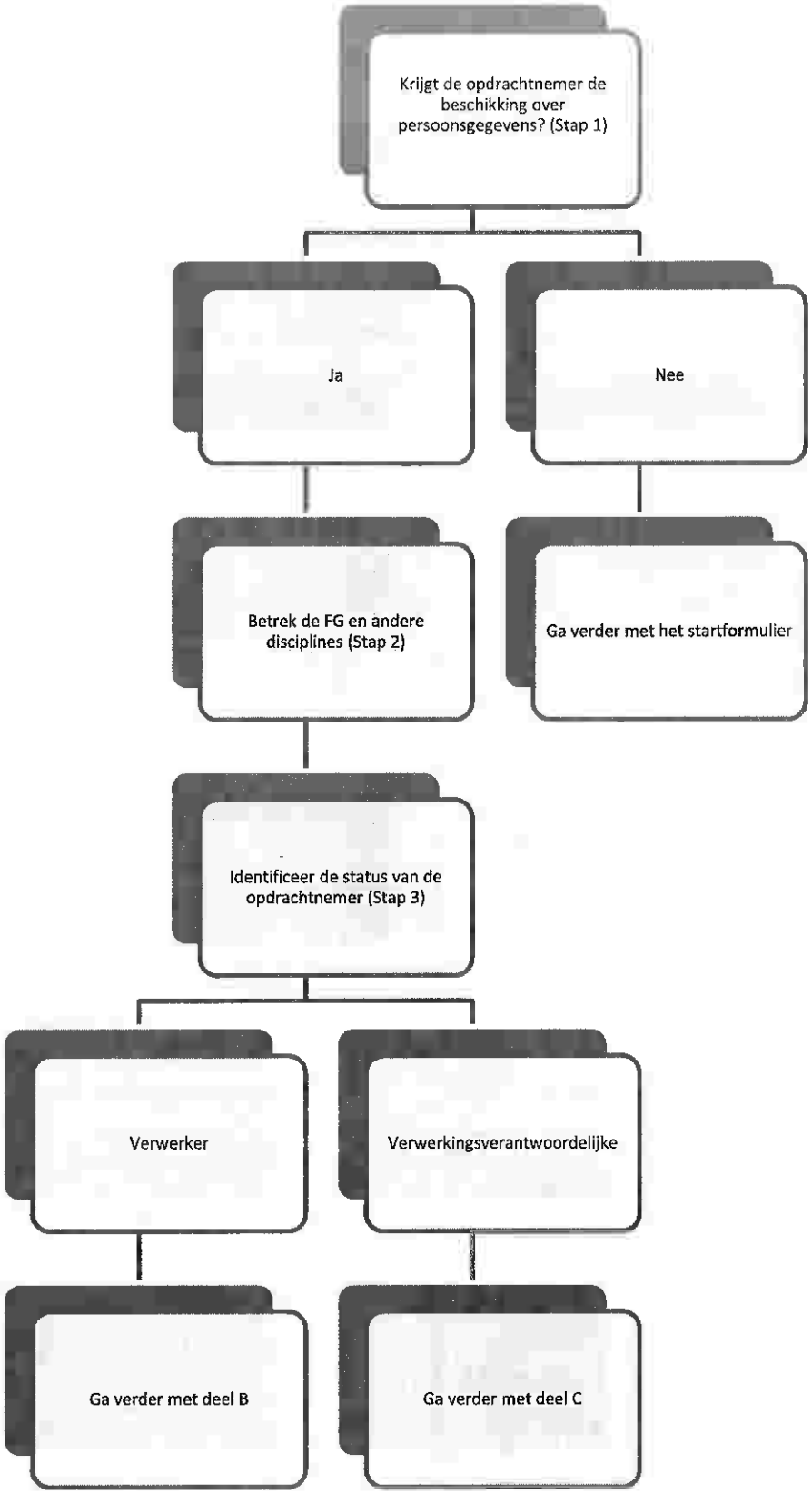
- de kans op het optreden van het risico als verwaarloosbaar wordt ingeschat;
- en/of de impact (de mogelijke schade) als aanvaardbaar wordt gezien;
- en/of de kwetsbaarheid verlagende maatregel als te kostbaar wordt ingeschat.

Deze notitie is geldig vanaf de datum van vaststelling. De CISO controleert jaarlijks de actualiteit van de beveiligingsmaatregelen en rapporteert hierover aan het Dagelijks Bestuur, als onderdeel van de P&C-cyclus. Mocht aan de hand van toekomstige risico analyses en/of incidenten blijken dat aanpassing van de geaccepteerde risico's aanpassing behoeft, dan wordt dit ter goedkeuring aan het Dagelijks Bestuur voorgelegd.

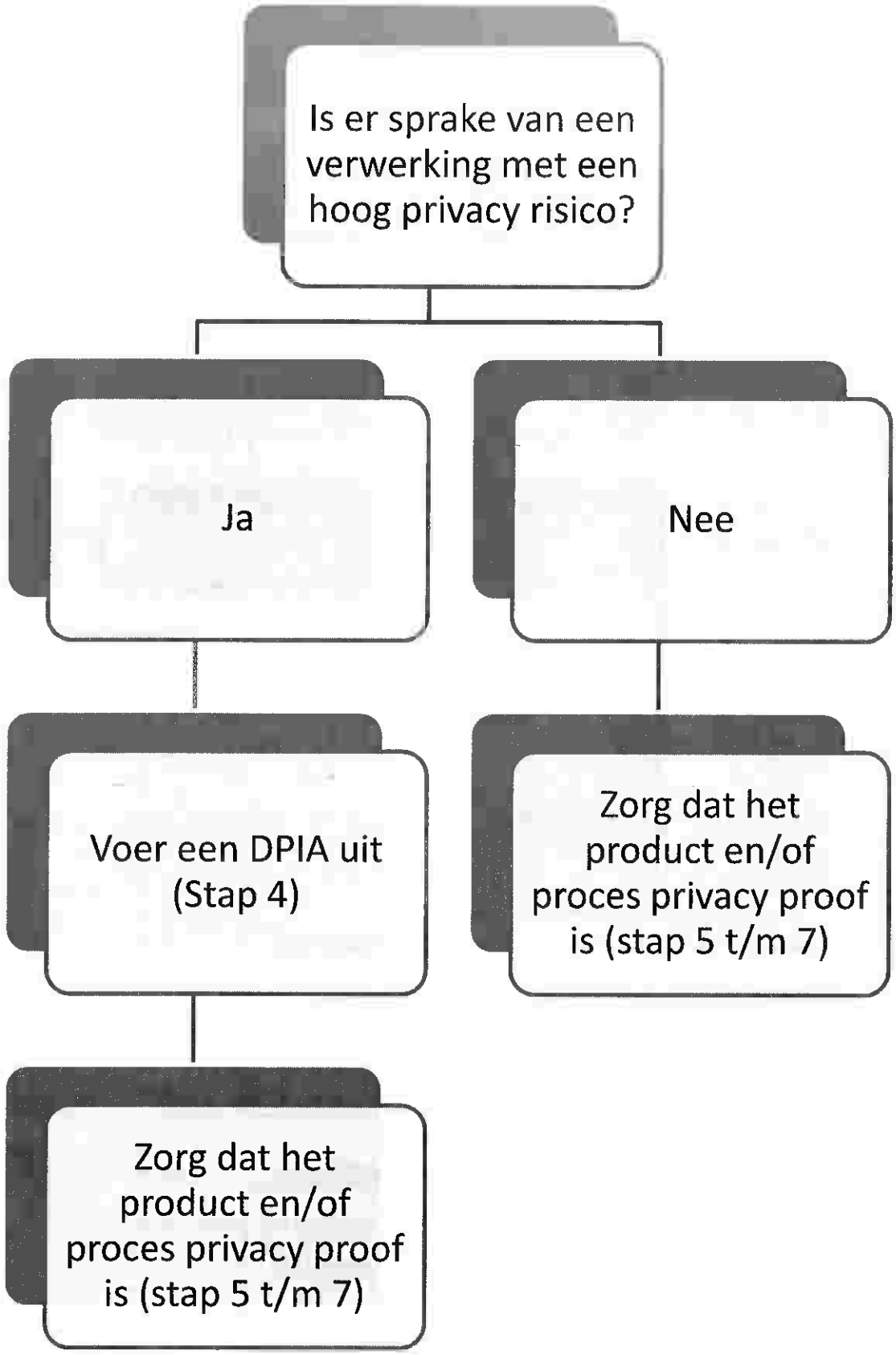
Bijlage:
Notitie 'Verklaring van Toepasselijkheid'.

Stappenplan: de AVG en het inkoopproces

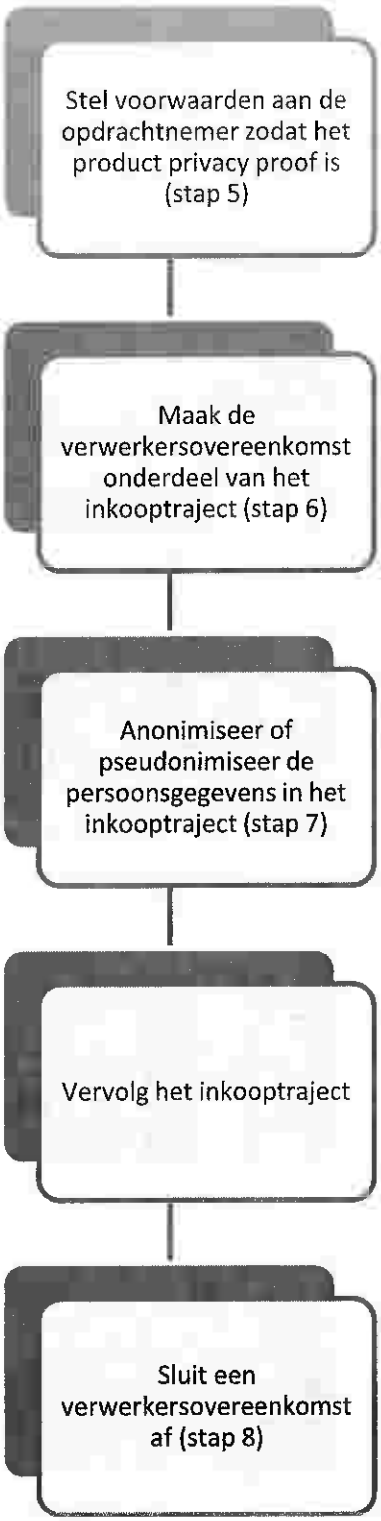
Deel A



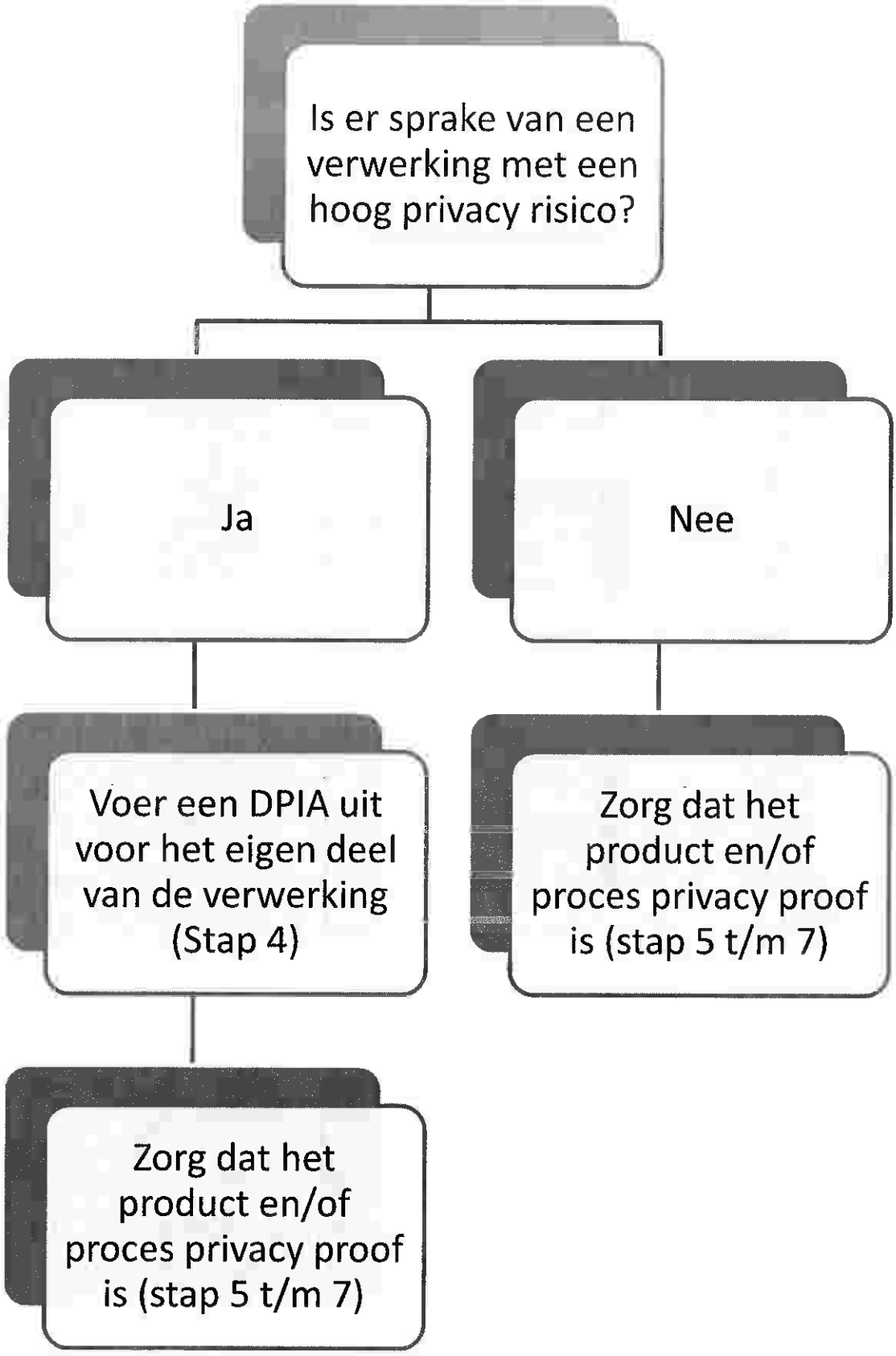
Deel B



Ga verder op de volgende pagina


Stel voorwaarden aan de opdrachtnemer zodat het product privacy proof is (stap 5)
Maak de verwerkersovereenkomst onderdeel van het inkooptraject (stap 6)
Anonimiseer of pseudonimiseer de persoonsgegevens in het inkooptraject (stap 7)
Vervolg het inkooptraject
Sluit een verwerkersovereenkomst af (stap 8)

Deel C



Ga verder op de volgende pagina


Stel voorwaarden aan de opdrachtnemer zodat het product privacy proof is (stap 5)
Anonimiseer of pseudonimiseer de persoonsgegevens in het inkooptraject (stap 7)
Vervolg het inkooptraject

'De AVG en het inkoopproces' (toelichting)

Zowel bij de inrichting als de uitvoering van het inkoop- en aanbestedingsproces draagt opdrachtgever er zorg voor dat bij de uitvoering van een opdracht wordt voldaan aan de eisen die voortvloeien uit de Algemene Verordening Gegevensbescherming (AVG) en de regelgeving op het gebied van informatiebeveiliging. Concreet houdt dit o.a. in dat:
- opdrachtgever voldoet aan de verplichtingen die de AVG oplegt aan de verstrekker van een opdracht waarbij persoonsgegevens worden verwerkt, bijvoorbeeld het sluiten van een verwerkersovereenkomst.
- opdrachtgever bij opdrachten met een ICT-component en/of waarbij persoonsgegevens worden verwerkt, met de leverancier afspraken maakt over een passend beveiligingsniveau. Bij de invulling van een passend beveiligingsniveau wordt met de leverancier een normenkader afgesproken als uitgangspunt, bijvoorbeeld NEN 7510, ISO27001/27002, BIG (Baseline Informatiebeveiliging Nederlandse gemeenten)
- Met de leverancier afspraken worden gemaakt met betrekking tot de beëindiging van de opdracht.

Dit document is te gebruiken als bijlage bij het gemeentelijke startformulier, maar ook zelfstandig door budgethouders, wanneer het startformulier niet hoeft te worden gebruikt. Deze toelichting maakt onderdeel uit van het stappenplan 'de AVG en het inkoopproces'

Toelichting bij deel A:

Stap 1. Inventariseer of opdrachtnemer beschikking krijgt over persoonsgegevens
In de voorbereiding van de offerteaanvraag is het belangrijk om te identificeren of de beoogde opdrachtnemer over persoonsgegevens zal beschikken. Persoonsgegevens zijn alle gegevens die te herleiden zijn naar een natuurlijke persoon. Als het antwoord daarop ja is, is de volgende stap om in kaart te brengen over welke informatie het gaat en of de opdrachtnemer zelf over de informatie beschikt of dat hij deze verkrijgt van de gemeente, de opdrachtgever. Op basis van bovenstaande informatie kan de opdrachtgever eisen stellen.

Stap 2. Betrek de Functionaris Gegevensbescherming (FG)
Wanneer de gemeente persoonsgegevens verstrekt aan de opdrachtnemer, betrek dan de FG. Dan kunnen de juiste eisen gesteld en de nodige maatregelen genomen worden. De FG kan ook controleren of de opdracht voldoet aan de gestelde eisen uit de AVG. Daarbij is het raadzaam om te beoordelen welke disciplines je nog meer nodig hebt voor het vervolgen van de inkoopprocedure, zoals ICT, informatiebeveiliging, inkoop en/of een inhoudelijk (beleids)medewerker.
Stap 3. Identificeer de status van opdrachtnemer
De volgende stap is in kaart brengen wie welke rol heeft in de gegevensverwerking. Dit is belangrijk omdat je als verantwoordelijke aansprakelijk bent voor schendingen, ook voor de schendingen door verwerkers. Er zijn twee rollen in de AVG:
• (verwerkings)verantwoordelijke: degene die het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt.
• verwerker: degene die ten behoeve van de verwerkingsverantwoordelijke persoonsgegevens verwerkt.

Op basis van de conclusies uit stap 3 kan je jouw rol als opdrachtgever identificeren.

Wanneer er in de inkoopprocedure sprake is van de relatie verwerkingsverantwoordelijke – verwerker: zie toelichting bij deel B.

Het is ook mogelijk dat meerdere organisaties verantwoordelijke zijn voor een deel van het proces. In dat geval zijn de organisaties medeverantwoordelijke. Zie hiervoor de toelichting deel C.

Toelichting bij deel B: De opdrachtnemer als verwerker

Stap 4. Voer zo nodig een DPIA uit
Onder de Algemene verordening gegevensbescherming (AVG) kunnen organisaties verplicht zijn een data protection impact assessment (DPIA) uit te voeren. Dat is een instrument om vooraf de privacyrisico's van een gegevensverwerking in kaart te brengen. En om daarna maatregelen te kunnen nemen om de risico's te verkleinen.

In de Nederlandse vertaling van de AVG wordt de term data protection impact assessment (DPIA) 'gegevensbeschermingseffectbeoordeling' genoemd.

Verplichte DPIA
Een DPIA is verplicht als een gegevensverwerking waarschijnlijk een hoog privacyrisico oplevert voor de betrokkenen over wie de organisatie gegevens verwerkt. Dit moet de verwerkingsverantwoordelijke zelf bepalen. U mag niet beginnen met het verwerken van gegevens voordat u een DPIA (en indien nodig een voorafgaande raadpleging) heeft uitgevoerd.

Risico bepalen
De AVG geeft aan dat er in ieder geval een DPIA moet worden uitgevoerd als een organisatie:
- systematisch en uitgebreid persoonlijke aspecten evalueert gebaseerd op geautomatiseerde verwerking, waaronder profiling, en daarop besluiten baseert die gevolgen hebben voor mensen;
- op grote schaal bijzondere persoonsgegevens verwerkt of strafrechtelijke gegevens verwerkt;
- op grote schaal en systematisch mensen volgt in een publiek toegankelijk gebied (bijvoorbeeld met cameratoezicht)

De Autoriteit Persoonsgegevens (toezichthouder op dit gebied) heeft een lijst gepubliceerd met categorieën van verwerkingen waarbij een DPIA verplicht is zie:
https://autoriteitpersoonsgegevens.nl/nl/zelf-doen/data-protection-impact-assessment-dpia#wat-zijn-de-criteria-van-de-ap-voor-een-verplichte-dpia-6667

De medewerker/het team dat inkoopt voert zelf een DPIA uit (evt. met behulp van een privacy officer of externe deskundige). De FG controleert vervolgens het rapport van de DPIA, om te beoordelen of het gevraagde product/proces aantoonbaar compliant is.

Stap 5. Stel aan het begin van het inkoopproces voorwaarden aan de opdrachtnemer en de opdracht zodat het product privacy proof is
Als verantwoordelijke is de gemeente ervoor verantwoordelijk dat de opdrachtnemer die verwerker is, voldoende garanties biedt dat de verwerking aan de AVG voldoet. Ook voor schendingen door verwerker is de gemeente aansprakelijk. De opdrachtnemer kan via de volgende middelen aantonen dat hij deze garanties biedt:

Verwerking persoonsgegevens beschreven in privacybijsluiter
Laat opdrachtnemer beschrijven van welke categorieën personen welke persoonsgegevens worden verwerkt in zijn dienst/product, en wat het doel is van deze verwerking.

> Toelichting:
> In de 'privacybijsluiter'[1] (bijlage .. bij de verwerkersovereenkomst) beschrijft de leverancier wat het doel is van de verwerking en welke persoonsgegevens worden verwerkt, zodat opdrachtgever kan bepalen of de verwerking zich beperkt tot het vervullen van zijn (wettelijke) ...taak. Opdrachtgever kan de informatie uit de bijsluiter onder meer gebruiken om betrokkenen adequaat te informeren.

Passende beveiligingsmaatregelen genomen
Opdrachtnemer maakt expliciet welke technische en organisatorische beveiligingsmaatregelen hij heeft genomen ter beveiliging van de door hem verwerkte persoonsgegevens, en hoe hij daarover zal rapporteren.

> Toelichting:
> Opdrachtnemer moet passende technische en organisatorische beveiligingsmaateregelen nemen. Hij beschrijft de maatregelen en de wijze van rapporteren (zoals in het geval van een datalek) in een

[1] Zoals bijlage 1 bij de model verwerkersovereenkomst van de VNG/IBD

productspecifieke bijlage[2] bij de verwerkersovereenkomst. Opdrachtgever moet kunnen vaststellen of zijn verantwoordelijkheid voldoende is vormgegeven.

Aantoonbaar compliant
Opdrachtnemer werkt mee aan een onderzoek door of namens opdrachtgever naar de mate waarin opdrachtnemer voldoet aan (beveiligings)eisen uit wet- en regelgeving en normen. Opdrachtnemer kan als vervanging van dit onderzoek een TPM (Third Party Medeling) overleggen om aan te tonen dat zijn organisatie aan de van toepassing zijnde eisen voldoet.[3]

Privacy en beveiliging meegenomen in het ontwerp
Opdrachtnemer volgt bij de inrichting van gegevensbeveiliging de principes van privacy by design en privacy by default.

Toelichting
Deze eis geldt tenminste voor nieuwe producten en de doorontwikkeling van bestaande producten.

Overdracht van gegevens uit administratie
Opdrachtnemer stelt de gegevens uit de administratie op verzoek ter beschikking van opdrachtnemer, in een standaard- of gebruikelijk gegevensformaat.

Toelichting
Opdrachtgever is verantwoordelijke, opdrachtnemer verwerker. Opdrachtgever moet naar eigen keuze kunnen veranderen van leverancier en daartoe gegevens kunnen migreren naar het systeem van de nieuwe leverancier. Opdrachtgever verwacht van de latende en ontvangende opdrachtnemer een zorgplicht, en een goede overdracht van de gegevens met een praktisch uitwisselingsformaat. De latende opdrachtnemer bewaart de gegevens tot opdrachtgever heeft aangegeven dat de overstap naar de nieuwe leverancier goed is verlopen. Opdrachtnemer treft zodanige maatregelen dat de gegevens ook bij een eventueel faillissement beschikbaar zijn voor overdracht.

Stap 6. Stel een verwerkingsovereenkomst op
Stel als voorwaarde het sluiten van een verwerkersovereenkomst. De verwerkingsverantwoordelijke is verplicht deze af te sluiten. Het is in feite een bijlage bij de hoofdovereenkomst. Maak gebruik van de modellen van VNG Realisatie, IBD / GIBIT.

Stap 7. Abstraheer en anonimiseer persoonsgegevens tot de noodzakelijke informatie in inkoopdocumenten
Tot slot is het belangrijk om geen privacygevoelige gegevens te delen in de aanbesteding zelf. Hanteer hierbij het principe 'need to know' voor alle stakeholders. Dat betreft zowel potentiele inschrijvers maar ook de leden van het inkoopteam. Het is niet nodig dat iedereen in het inkoopteam inzicht heeft in alle gegevens van een aanbesteding, vooral niet als het om persoonsgegevens gaat. Voor het inkoopteam is relevant wie welke gegevens nodig heeft om goede input te leveren aan de aanbestedingsdocumenten. Ook voor de inschrijvers geldt dat persoonsgegevens vaak niet nodig zijn voor het indienen van een offertes. Vaak kunnen de gegevens tot een dusdanig abstractieniveau worden gebracht zodat de gegevens anoniem zijn.

Privacy tijdens de inkoopprocedure
Ook als de offerteaanvraag gedaan is, is het in de vragenronde belangrijk om alert te zijn dat je geen aanpassingen doet waardoor je niet meer aan de AVG verplichtingen kan voldoen. Een risico zit in een klein hoekje. Zo is het mogelijk dat je onbewust akkoord gaat met een andere invulling van beveiliging of een beperking van auditbepalingen, waardoor het niet meer mogelijk is om effectief te toetsen of de opdrachtnemer aan de AVG voldoet. Als verantwoordelijke opdrachtgever heb jij wel die verplichting. Tegelijkertijd geldt ook in deze fase dat ook het 'need to know' principe voor het inkoopteam. Bij bijvoorbeeld inhuur van personeel ontvang je van inschrijvers persoonsgegevens over kandidaten. Het is het niet noodzakelijk dat degenen die beoordelen beschikken over de adresgegevens en bereikbaarheidsgegevens van kandidaten.

Stap 8. Sluit een verwerkingsovereenkomst af
Wanneer de procedure succesvol is afgerond en resulteert in het afsluiten van de hoofdovereenkomst met de marktpartij dan is het zaak om de verwerkersovereenkomst daadwerkelijk af te sluiten. Stel je FG hiervan op de hoogte, voor het aanpassen van het register van verwerkingsactiviteiten.

---

[2] Zoals bijlage 2 bij de model verwerkersovereenkomst van de VNG/IBD

[3] Zoals in bijlage 2 bij de model verwerkersovereenkomst van de VNG/IBD

Houdt revisie van de afspraken in het vizier en voer dan het stappenplan opnieuw (summier) uit.

Privacy tijdens de uitvoering van het contract
Ook na het afsluiten van het contract, sterker nog, juist na dit moment is het noodzakelijk om de naleving AVG goed te bewaken. Dit is alleen mogelijk met proactief contractmanagement. De contractmanager dient te zorgen dat de afspraken worden nageleefd. Voorbeelden zijn of ISO-certificeringen of andere geëiste certificeringen up-to-date zijn en of de opdrachtnemer nog steeds gebruik maakt van een dataserver in de EU (of andere AVG conform land). Wanneer de opdrachtnemer de AVG gerelateerde afspraken niet naleeft, heeft de contractmanager de juiste bevoegdheden nodig om bijvoorbeeld boetes op te kunnen leggen. Tot slot is noodzakelijk dat zij de inhoud van het contract, inclusief de AVG gerelateerde afspraken goed doorgronden. Hierbij helpt het onderhouden van een goede intensieve relatie met de Functionaris Gegevensbescherming en geregeld overleg met de opdrachtnemer over privacy.

Privacy na het uitvoeren contract
Na wijziging (toevoeging, uitbreiding) van het product of de dienst is het belangrijk om zo nodig opnieuw een DPIA uit te voeren en een nieuwe verwerkersovereenkomst bij het nieuwe contract af te sluiten.

Toelichting bij deel C : Partij is verwerkingsverantwoordelijke

Het komt ook voor dat beide partijen verwerkingsverantwoordelijke zijn. Gezamenlijk voor het geheel of ieder voor een deel van de verwerking. In het eerste geval zal er geen sprake zijn van een inkoopprocedure. Als medeverantwoordelijke ben je voor de wet ook verantwoordelijk voor het geheel, en kan je dus aansprakelijk worden gesteld voor schendingen van andere medeverantwoordelijken, tenzij je kan bewijzen dat je niets van doen hebt met de schending. Het is dus verstandig om in een soort partnerschap concrete afspraken met elkaar te maken (bijv. convenant). Ook is het belangrijk om dan oog te hebben voor de eventuele verplichting om een DPIA uit te voeren. Bij gegevensuitwisseling moet onderzocht worden welke gegevens verstrekt mogen worden. Dit kan vastgelegd worden in een gegevensuitwisselingsovereenkomst. Hierin neem je afspraken op over wat er van elkaar verwacht wordt, zoals: wat moet er op een factuur staan? Pas op dat je hier geen verplichtingen voor de andere partij opneemt over het verwerken van de persoonsgegevens. Dan lijkt het alsof er een verwerkersrelatie wordt nagebootst en neem je meer verantwoordelijkheid op je dan beoogd is.

In het tweede geval, wanneer je beiden voor een deel van het proces verantwoordelijk bent, is er vaak wél sprake van een inkoopsituatie. Bijvoorbeeld bij de inkoop van Wmo hulpmiddelen. Het college is verwerkingsverantwoordelijk voor het proces van de aanvraag en de toekenning van het recht op het hulpmiddel. De organisatie die de hulpmiddelen levert is verantwoordelijk voor het leveren van het product.

In deze situatie regel je dus:

- geen verwerkersovereenkomst;
- stel je wel voorwaarden aan het product of dienst. Je koopt dus privacy proof in;
- dat een eventuele DPIA alleen voor je eigen gedeelte van het proces wordt uitgevoerd;
- beoordeel je welke persoonsgegevens verstrekt mogen worden aan de opdrachtnemer.

Bezoek de volgende websites voor meer achtergrondinformatie:

- www.autoriteitpersoonsgegevens.nl
- www.vngrealisatie.nl
- https://www.cip-overheid.nl/wp-content/uploads/2018/04/20180415-Security-Proof-Inkopen-2pager-1.pdf

Algemene Inkoop voorwaarden voor leveringen en diensten Stadsbank Oost Nederland 2018

Inhoudsopgave

I Algemeen

Artikel 1 Definities

Aflevering:	het verschaffen van het bezit van de Goederen aan de Stadsbank
Contractant:	de in de Overeenkomst genoemde wederpartij van de Stadsbank
Diensten (Dienst):	de door de Contractant te verrichten werkzaamheden ten behoeve van een specifieke behoefte van de Stadsbank, niet zijnde werken of leveringen
Stadsbank:	de gemeenschappelijke regeling Stadsbank Oost Nederland, zetelend Spelbergsweg 35-37 te Enschede
Goederen:	alle zaken en alle vermogensrechten in de zin van artikel 3:1 Burgerlijk Wetboek
Leveringen (Levering):	de door de Contractant op basis van de Overeenkomst ten behoeve van de Stadsbank te leveren Goederen
Offerte:	een aanbod in de zin van het Burgerlijk Wetboek
Offerteaanvraag:	een enkelvoudige of meervoudige aanvraag van de Stadsbank voor te verrichten Prestaties of een (Europese) aanbesteding conform de Aanbestedingswet1 en de Europese aanbestedingsrichtlijnen 2004/17/EG en 2004/18/EG
Overeenkomst:	al hetgeen tussen de Stadsbank en de Contractant is overeengekomen, inclusief daarbij behorende bijlagen
Partijen/Partij:	de Stadsbank en/of de Contractant
Personeel van Contractant:	de door de Contractant voor de uitvoering van de Overeenkomst in te schakelen personeelsleden of andere hulppersonen die krachtens de Overeenkomst onder zijn verantwoordelijkheid werkzaam zullen zijn
Prestatie:	de te verrichten Leveringen en/of Diensten
Werkdag:	kalenderdagen behoudens weekenden, algemeen erkende feestdagen in de zin van artikel 3 lid 1 Algemene termijnenwet, plaatselijke feestdagen en door de Stadsbank aangewezen brugdagen

Artikel 2 Toepasselijkheid

2.1. Deze algemene inkoopvoorwaarden zijn van toepassing op de Offerteaanvraag en Overeenkomsten met betrekking tot Leveringen en Diensten.

2.2. Bij alle inkopen en aanbestedingen op het gebied van IT zijn, aanvullend op deze algemene inkoopvoorwaaarden, de actuele Gemeentelijke Inkoopvoorwaarden bij IT (GIBIT) van toepassing.

2.3. Van deze algemene inkoopvoorwaarden kan slechts worden afgeweken, indien Partijen dit uitdrukkelijk schriftelijk met elkaar zijn overeengekomen.

2.4. Indien een bepaling van deze algemene inkoopvoorwaarden nietig is of vernietigd wordt, zullen de overige bepalingen van kracht blijven en treden Partijen in overleg teneinde een nieuwe bepaling (of bepalingen) ter vervanging van de nietige of vernietigde bepaling(en) overeen te komen, waarbij zoveel mogelijk het doel en de strekking van de nietige of vernietigde bepaling(en) in acht worden genomen.

2.5. Door het indienen van de Offerte wijst de Contractant uitdrukkelijk de toepasselijkheid van zijn algemene voorwaarden af.

Artikel 3 Offerte, opdracht en totstandkoming Overeenkomst

3.1. De Stadsbank kan een Offerteaanvraag intrekken of wijzigen Voor zover dit mogelijk is binnen de geldende Nederlandse en Europese jurisprudentie en wet- en regelgeving. De Stadsbank zal geen kosten of schade vergoeden die hiermee samenhangen, tenzij schriftelijk anders is overeengekomen.

3.2. De Offerte van de Contractant heeft een gestanddoeningstermijn van negentig dagen of zoveel langer of korter als in de Offerteaanvraag is vermeld. De gestanddoeningstermijn vangt aan op de dag waarop de inschrijvingstermijn sluit of op de dag die wordt vermeld in de Offerteaanvraag.

3.3. Een Overeenkomst komt tot stand nadat de Stadsbank een expliciete schriftelijke aanvaarding van de Offerte van de Contractant per e-mail, fax of brief heeft verzonden aan de Contractant. De schriftelijke aanvaarding geldt enkel als aanvaarding, indien daaraan een besluit ten grondslag ligt als bedoeld in artikel 33b, eerste lid aanhef en onder e van de Wet gemeenschappelijke regelingen dat is genomen door of namens het Dagelijks Bestuur en de aanvaarding ondertekend is door de Voorzitter of een ander waaraan op grond van het bepaalde in artikel 33d, tweede lid van de Wet gemeenschappelijke regelingen de vertegenwoordiging van de Stadsbank is opgedragen. Op eerste verzoek van de Contractant legt de Stadsbank een kopie van dit besluit over.

3.4. Een voornemen tot gunning houdt geen aanvaarding in zoals bedoeld in het voorgaande lid of in de zin van artikel 6:217 lid 1 Burgerlijk Wetboek.

3.5. Alle handelingen die de Contractant verricht voorafgaand aan de totstandkoming van de Overeenkomst zijn voor rekening en risico van de Contractant.

II Uitvoering overeenkomst

Artikel 4 Algemene verplichtingen Contractant

4.1. De Contractant zal zijn verplichtingen voortvloeiend uit de Overeenkomst in nauwe samenwerking met de Stadsbank nakomen, onverminderd de eigen verantwoordelijkheid van de Contractant.

4.2. De Contractant zal de Stadsbank op de hoogte houden van de uitvoering van de Overeenkomst en desgevraagd inlichtingen geven. De Contractant is onder meer, doch niet uitsluitend, verplicht om de Stadsbank direct schriftelijk in te lichten over feiten en omstandigheden die kunnen leiden tot vertraging in de nakoming of waarmee in de Overeenkomst geen rekening is gehouden.

4.3. Slechts met voorafgaande schriftelijke goedkeuring van de Stadsbank, kan de Contractant de uitvoering van de Overeenkomst geheel of gedeeltelijk laten uitvoeren door derden of uit de Overeenkomst voortvloeiende rechten en/of plichten overdragen aan derden.

4.4. De Contractant garandeert ter zake van de Overeenkomst dat de Contractant of Personeel van Contractant of een met de Contractant verbonden rechtspersoon en de onder hen werkzame personen niet betrokken zijn of zijn geweest bij overleg of afspraken met andere ondernemingen op een wijze die strijdig zou kunnen zijn met bepalingen van de Mededingingswet of artikelen 101 en 102 Verdrag betreffende de werking van de Europese Unie, waaronder: (1) prijsvorming, (2) het afstemmen van Offerten, en/of (3) verdeling van werkzaamheden.

4.5. De Contractant vrijwaart de Stadsbank voor strafrechtelijke boetes en bestuurlijke sancties (als bedoeld in artikel 5:2, eerste lid aanhef en onder a van de Algemene wet bestuursrecht, het eventuele kostenverhaal daaronder begrepen) die verband houden met de Overeenkomst en die de Contractant of de Stadsbank krijgt opgelegd.

4.6. De Contractant zal bij de uitvoering van de Overeenkomst alle van toepassing zijn de voorschriften bij of krachtens de wet gesteld naleven en de overeenkomsten die de Stadsbank met derden heeft gesloten, voor zover deze overeenkomsten bekend zijn bij de Contractant, in acht nemen. Indien de Contractant genoodzaakt is om contact op te nemen met derden, zal de Contractant dit eerst voorleggen aan de Stadsbank.

4.7. De Contractant draagt zelf de verantwoordelijkheid om de door hem ingeschakelde derden te informeren over de afspraken die gelden tussen de Contractant en de Stadsbank bij de uitvoering van de Overeenkomst.

4.8. Slechts voor zover de Contractant expliciet en schriftelijk is gemachtigd door de Stadsbank zal de Contractant optreden als gemachtigde van de Stadsbank. Eventuele gevolgen die door het in strijd handelen met het bepaalde in de voorgaande zin zijn ontstaan, komen voor rekening en risico van de Contractant.

Artikel 5 Algemene verplichtingen Stadsbank

5.1. De Stadsbank zal op verzoek van de Contractant alle inlichtingen en gegevens verstrekken voor zover die nodig zijn om de Overeenkomst naar behoren uit te voeren.

5.2. De Stadsbank zal zich inspannen zoals een goed opdrachtgever betaamt en zal zich indien nodig inspannen om haar medewerking, waaronder publiekrechtelijke medewerking, te verlenen die nodig zou kunnen zijn voor de uitvoering van de Overeenkomst.

Artikel 6 Kwaliteit, keuring en garantie

6.1. De Contractant garandeert dat de geleverde Prestaties voldoen aan de Overeenkomst, aan de algemeen geldende normen en aan de voorschriften die bij of krachtens wet of verdrag gelden met betrekking tot, doch niet uitsluitend, veiligheid, gezondheid en milieu.

6.2. De Stadsbank is gerechtigd om de Prestaties te keuren en de Contractant verleent waar nodig zijn medewerking. Indien de Stadsbank bepaalde Prestaties schriftelijk heeft goedgekeurd, vervalt het recht zoals genoemd in de voorgaande zin ten aanzien van die Prestaties.

Artikel 7 Geheimhouding

7.1. Partijen verplichten zich om al wat bij de uitvoering van de Overeenkomst ter kennis komt en waarvan het vertrouwelijke karakter bekend is of redelijkerwijs kan worden vermoed, op generlei wijze bekend te maken - inclusief via kanalen van sociale media - of voor eigen doeleinden te gebruiken, behalve voor zover enig wettelijk voorschrift of rechterlijke uitspraak tot bekendmaking noopt.

7.2. Partijen zullen de onder hen werkzame personen of door hen ingeschakelde derden verplichten deze geheimhoudingsplicht na te leven.

7.3. Partijen hebben het recht om in geval van overtreding van de voorgaande leden door de andere Partij en/of de voor die Partij werkzame personen en/of door die Partij ingeschakelde derden de Overeenkomst per direct op te schorten dan wel zonder rechterlijke tussenkomst en zonder ingebrekestelling te ontbinden. Elke opschorting dan wel ontbinding geschiedt door middel van een aangetekend schrijven.

7.4. De Contractant is verplicht om op eerste verzoek van de Stadsbank Personeel van Contractant een geheimhoudingsverklaring te laten ondertekenen.

Artikel 8 Intellectueel eigendom

8.1. Alle (aanspraken op) intellectuele eigendomsrechten (IE-rechten) met betrekking tot enig resultaat voortvloeiende uit de Overeenkomst, berusten bij de Stadsbank, tenzij schriftelijk anders is overeengekomen. De Contractant draagt deze (aanspraken op) IE-rechten – voor zover nodig – om niet over aan de

Stadsbank. De Contractant zal op eerste verzoek kosteloos meewerken aan het bewerkstelligen van de overdracht.

8.2. Onder resultaat als bedoeld in lid 1 van dit artikel, wordt verstaan al hetgeen in het kader van de Overeenkomst tot stand wordt gebracht ongeacht of de Contractant daarbij gebruik maakt van enige bijdrage van de Stadsbank en/of derden.

8.3. De Contractant doet voor zover mogelijk afstand van alle eventuele persoonlijkheidsrechten op in het kader van de Overeenkomst tot stand gebrachte auteursrechtelijke werken.

8.4. Tenzij schriftelijk anders is overeengekomen, behoudt of verkrijgt de Contractant geen gebruiksrecht met betrekking tot enig resultaat van de Overeenkomst.

8.5. De Stadsbank behoudt zich uitdrukkelijk het auteursrecht voor met betrekking tot ieder in het kader van de Overeenkomst aan Contractant openbaar gemaakt werk. De Contractant erkent dit voorbehoud.

8.6. De Contractant garandeert dat de gekochte Goederen en toebehoren alsmede de geleverde Diensten en al hetgeen daarmee gepaard gaat of daaruit resulteert vrij zijn van alle bijzondere lasten en beperkingen die aan het vrije gebruik daarvan door de Stadsbank in de weg zouden kunnen staan, zoals octrooirechten, merkrechten, modelrechten of auteursrechten en vrijwaart de Stadsbank tegen alle aanspraken van derden dienaangaande.

8.7. In het geval van aanspraken van derden zal de Contractant alles in het werk stellen om in overleg met de Stadsbank te bewerkstelligen dat de Stadsbank het ongestoorde gebruik van het geleverde zal kunnen voortzetten.

8.8. In het geval van aanspraken van derden waarvoor de hierboven genoemde vrijwaringverplichting geldt, zal de Contractant alle schade van de Stadsbank vergoeden inclusief proceskosten, waaronder tevens begrepen redelijke advocaatkosten voor het voeren van gerechtelijke procedures.

Artikel 9 Wijziging Overeenkomst

9.1. De Stadsbank is bevoegd om de Overeenkomst schriftelijk te wijzigen en/of aan te vullen, na overleg met en instemming van de Contractant over de gevolgen van de wijziging of aanvulling.

9.2. In dit kader blijven Partijen binnen de grenzen van de redelijkheid en billijkheid.

Artikel 10 Uitrusting en materialen

10.1. De Contractant zal voor eigen rekening en risico zorg dragen voor alle bij de uitvoering van de Overeenkomst te gebruiken - niet van de Stadsbank afkomstige - materialen en uitrusting (waaronder gereedschappen), tenzij schriftelijk anders is overeengekomen.

10.2. De Contractant is verantwoordelijk en aansprakelijk voor de deugdelijkheid van de gebruikte Goederen, materialen en uitrusting en dient deze voor eigen rekening en risico te verzekeren, tenzij schriftelijk anders is overeengekomen.

Artikel 11 Tijdstip van nakoming

11.1. De Contractant is van rechtswege in verzuim nadat de fatale termijn(en) of termijnen voor de uitvoering van de desbetreffende Prestaties, zoals vermeld in de Overeenkomst, zijn verstreken en de desbetreffende Prestaties niet of niet volledig zijn uitgevoerd.

11.2. De Contractant stelt de Stadsbank schriftelijk tijdig en met opgaaf van redenen in kennis van een eventuele vertraging en de maatregelen die de Contractant zal treffen om de vertraging zoveel mogelijk te beperken.

Artikel 12 Toerekenbare tekortkoming

12.1 Indien één van de Partijen toerekenbaar tekort schiet in de nakoming van de Overeenkomst en/of deze algemene inkoopvoorwaarden, zal de andere Partij een aangetekend schrijven verzenden aan de tekortkomende Partij, alvorens gebruik te maken van de Partij toekomende wettelijke rechten, behoudens de gevallen waarin ingebrekestelling ingevolge het Burgerlijk Wetboek achterwege kan blijven, in welke gevallen de nalatige Partij direct in verzuim verkeert.

12.2. Ieder der Partijen is gerechtigd de Overeenkomst zonder rechterlijke tussenkomst en zonder ingebrekestelling met onmiddellijke ingang te ontbinden, indien de andere Partij in verzuim is geraakt, behoudens voor zover ontbinding – gelet op de omstandigheden van het geval, waaronder de ernst van het verzuim – in strijd zou zijn met de redelijkheid en billijkheid. Elke ontbinding geschiedt door middel van een aangetekend schrijven.

12.3. Er is geen sprake van enige toerekenbare tekortkoming zijdens de Stadsbank indien en voor zover de publiekrechtelijke verantwoordelijkheid noopt tot het niet verstrekken van inlichtingen en gegevens respectievelijk tot het niet verlenen van de publiekrechtelijke medewerking die nodig zou kunnen zijn voor de uitvoering van de Overeenkomst.

Artikel 13 Niet toerekenbare tekortkoming

13.1. De Contractant kan zich jegens de Stadsbank enkel op overmacht beroepen, indien de Contractant de Stadsbank zo spoedig mogelijk, onder overlegging van de bewijsstukken, schriftelijk van het beroep op overmacht in kennis stelt.

Artikel 14 Aansprakelijkheid en verzekering

14.1. De Contractant vrijwaart de Stadsbank tegen eventuele aanspraken van derden terzake van schade door deze derden geleden ten gevolge van de uitvoering door de Contractant van de Overeenkomst en het gebruik of toepassing van de geleverde Goederen of Diensten van de Contractant.

14.2. De Contractant zal vanaf het aangaan van de Overeenkomst adequaat verzekerd zijn voor het uitvoeren van de Overeenkomst en zal zich adequaat verzekerd houden gedurende de uitvoering van de Overeenkomst.

14.3. De Contractant zal het verzekerd bedrag en de polisvoorwaarden gedurende de uitvoering van de Overeenkomst niet ten nadele van de Stadsbank wijzigen, tenzij de Stadsbank hiervoor haar expliciete en schriftelijke toestemming heeft gegeven.

14.4. Eventuele verzekeringen die noodzakelijk zijn in het kader van de uitvoering van de Overeenkomst en waarover de Contractant nog niet beschikt, zal de Contractant afsluiten tenminste voor de periode van de uitvoering van de Overeenkomst.

Artikel 15 Boete

15.1. Indien een boetebepaling is overeengekomen, is deze boete zonder rechterlijke tussenkomst, ingebrekestelling of aanmaning direct opeisbaar.

15.2. De boete laat onverlet alle andere rechten of vorderingen, waaronder, doch niet uitsluitend, de vordering van de Stadsbank tot nakoming en het recht op schadevergoeding.

Artikel 16 Toepasselijk recht en geschillen

16.1. Op deze algemene inkoopvoorwaarden en de Overeenkomsten, alsmede op de totstandkoming en de interpretatie, is Nederlands recht van toepassing.

16.2. De toepasselijkheid van het Weens Koopverdrag (United Nations Convention on Contracts for the International Sale of Goods) wordt uitdrukkelijk uitgesloten.

16.3. Als er een geschil ontstaat met betrekking tot de Offerteaanvraag, de procedure zoals beschreven in de Offerteaanvraag, de totstandkoming van de Overeenkomst of de uitvoering van de Overeenkomst, dan is elk der Partijen gerechtigd om het geschil voor te leggen aan de bevoegde rechter in het arrondissement waar de Stadsbank gevestigd is.

III Financiële bepalingen

Artikel 17 Prijzen, meerwerk en minder werk

17.1. De Contractant zal de Overeenkomst uitvoeren tegen de in zijn Offerte genoemde prijzen in Euro's.

17.2. Niet redelijkerwijs in de Overeenkomst inbegrepen extra Prestaties, zijn slechts meerwerk voor zover dit uitsluitend aan de Stadsbank is toe te rekenen.

17.3. Meerwerk zal door de Contractant slechts in behandeling worden genomen nadat de inhoud en het budget schriftelijk zijn overeengekomen met de Stadsbank.

17.4. Verrekening van meerwerk of minder werk vindt plaats tegen maximaal de tarieven zoals opgenomen in de Offerte, tenzij schriftelijk anders is overeengekomen.

17.5. Voor zover prijzen en tarieven van meerwerk of minder werk niet in de Offerte zijn opgenomen, verplicht de Contractant zich ertoe voor meerwerk en minder werk uitsluitend marktconforme tarieven aan te bieden.

Artikel 18 Facturering en betaling

18.1. Op de factuur vermeldt de Contractant;

- de wettelijke vereisten waaraan de factuur moet voldoen:
  naam, adres, postcode, woonplaats, bank/gironummer en de benodigde IBAN- en BIC-gegevens, BTW-nummer, KvK-nummer;
- het factuuradres van de Contractant;
- het totale factuurbedrag inclusief en exclusief BTW; *en*
- eventuele nadere eisen in overleg met de Stadsbank.

18.2. De Contractant hanteert een betalingstermijn van dertig dagen na de ontvangst van de factuur of zoveel langer of korter als overeengekomen tussen Partijen in de Overeenkomst. De Stadsbank zal binnen de gehanteerde betalingstermijn de factuur van de Contractant betalen.

18.3 Indien de Goederen of Diensten niet beantwoorden aan de Overeenkomst is de Stadsbank bevoegd om de betaling naar rato van de tekortkoming geheel of gedeeltelijk op te schorten.

IV Bepalingen betreffende de leveringen van goederen

Artikel 19 Leveringen

19.1. De Contractant levert de Goederen conform Delivered Duty Paid (DDP), volgens Incoterms 2010, zoals vastgesteld door de Internationale Kamer van Koophandel (ICC).

19.2. Tenzij schriftelijk een andere tijd of plaats is overeengekomen, geschiedt de Aflevering uitsluitend op Werkdagen tijdens de openingsuren van het Stadsbank. De Contractant dient zijn vervoerder hiervan op de hoogte te stellen.

19.3. Indien de Stadsbank de Goederen gemotiveerd afkeurt, zal de Contractant op zijn eigen kosten de Goederen ophalen.

19.4. De Goederen worden geacht te zijn goedgekeurd vanaf het moment van volledige operationele ingebruikname door de Stadsbank, tenzij schriftelijk anders is overeengekomen of bepaalde omstandigheden nopen tot schriftelijke goedkeuring van de Stadsbank.

19.5. De Contractant verleent tenminste een garantie voor de Goederen van twaalf maanden vanaf het moment dat de Stadsbank de Goederen heeft goedgekeurd, tenzij schriftelijk anders is overeengekomen. Deze garantie laat onverlet de aansprakelijkheid van de Contractant.

19.6. De Contractant garandeert dat voor een periode van tenminste vijf jaar of een termijn die schriftelijk is overeengekomen na Aflevering van de Goederen, onderdelen van de Goederen kunnen worden geleverd.

19.7. De Contractant is gehouden om alle bij de Goederen behorende gebruiksaanwijzingen en productinformatie, alsmede eventuele kwaliteitskeurmerken of -certificaten, opgesteld zoveel mogelijk in de Nederlandse taal, zonder additionele kosten, aan de Stadsbank ter beschikking te stellen.

19.8. De Contractant zal voor zijn rekening en risico alle voorkomende gebreken aan de geleverde Goederen na Aflevering of voltooiing binnen de door de Stadsbank bij eerste aanzegging gestelde redelijke termijn wegnemen door herstel of vervanging.

Artikel 20 Verpakking en transport

20.1. De Contractant draagt zorg voor een deugdelijke verpakking, alsmede voor een zodanige beveiliging en vervoer van de Goederen, dat deze in een goede staat de plaats van Aflevering bereiken en het lossen daar veilig kan plaatsvinden. De Contractant is verantwoordelijk voor het naleven van de Nederlandse, Europese en internationale voorschriften met betrekking tot verpakkingen.

20.2. De Contractant neemt alle verpakkingen kosteloos terug, tenzij schriftelijk anders is overeengekomen.

Artikel 21 Overdracht van eigendom en risico

21.1. De eigendom van de geleverde Goederen gaat over op het moment van Aflevering, waar nodig na eventuele installatiewerkzaamheden die daarmee gepaard gaan. Het risico gaat over op de Stadsbank na acceptatie van de Goederen door de Stadsbank.

21.2. De acceptatie van de Goederen zal geschieden door middel van een schriftelijke verklaring van de Stadsbank, na Aflevering en eventuele installatie van de Goederen. Indien de Stadsbank de Goederen niet accepteert, geeft zij gemotiveerd aan waarom de acceptatie onthouden wordt.

V Bepalingen betreffende het verrichten van diensten

Artikel 22 Diensten

22.1. De Contractant zal de Diensten uitvoeren binnen de termijn en op de plaats zoals deze zijn opgenomen in de Overeenkomst.

22.2. De Contractant draagt de volledige verantwoordelijkheid voor zowel zijn eigen Prestaties, Prestaties van Personeel van Contractant alsmede Prestaties van de door de Contractant ingeschakelde derden.

22.3. Feitelijke uitvoering van de Diensten door de Contractant of daarmee gepaard gaande handelingen houdt niet in dat de Stadsbank de Diensten zonder meer goedkeurt. De Stadsbank behoudt zich het recht voor om eventuele verrichtte Diensten te keuren, controleren of niet goed te keuren.

22.4. De goedkeuring van de Diensten zal geschieden door middel van een schriftelijke verklaring van de Stadsbank. Indien de Stadsbank de Diensten niet goedkeurt, geeft zij gemotiveerd aan waarom de goedkeuring onthouden wordt.

Artikel 23 Personeel van Contractant

23.1. Voor zover Diensten worden verricht ten kantore en/of in de openbare ruimte van de Stadsbank, zijn de Contractant, Personeel van Contractant en de door de Contractant ingeschakelde derden gehouden de vastgestelde huisregels voor dat kantoor/gebouw en/of die openbare ruimte na te leven.

23.2. Indien gedurende de uitvoering van de Overeenkomst blijkt dat Personeel van Contractant niet functioneert in het belang van de goede uitvoering van de Overeenkomst en/of wegens omstandigheden zijn werkzaamheden niet kan voortzetten, dan heeft de Stadsbank het recht de desbetreffende persoon door de Contractant te laten vervangen.

23.3. Voor de vervanging van Personeel van Contractant is voorafgaande schriftelijke toestemming vereist van de Stadsbank, tenzij directe vervanging van Personeel van Contractant noodzakelijk is. In dat laatste geval kan worden volstaan met mondelinge toestemming van de Stadsbank. Uitgangspunt daarbij is dat personen beschikbaar worden gesteld die een vergelijkbare deskundigheid, opleiding en ervaring hebben (conform het vereiste in de Offerteaanvraag).

23.4. Vervanging van Personeel van Contractant wordt op een korte termijn – doch uiterlijk binnen twee weken of zoveel korter als noodzakelijk – door de Contractant voorzien. Eventuele kosten die gepaard gaan met vervanging komen voor rekening van de Contractant.

23.5. De Contractant staat ervoor in dat het Personeel van Contractant gerechtigd is om in Nederland arbeid te verrichten dan wel Diensten te verrichten.

23.6. De Contractant is verantwoordelijk voor en aansprakelijk voor de nakoming van de uit de Overeenkomst voortvloeiende verplichtingen uit de belastingwetgeving en de sociale zekerheidswetgeving, waaronder begrepen verplichtingen die verband houden met het Uitvoeringsinstituut Werknemersverzekeringen (UWV).

De Contractant vrijwaart de Stadsbank tegen alle aanspraken terzake. De Contractant zal - indien wettelijk vereist dan wel door de Stadsbank wordt vereist - met een G-rekening werken. Indien de Stadsbank geconfronteerd wordt met een naheffing, worden deze kosten een–op-een verhaald op de Contractant.

VI Einde overeenkomst

Artikel 24 Opzegging

24.1. De Stadsbank is gerechtigd de Overeenkomst op te zeggen met inachtneming van een opzegtermijn zoals bepaald in de Overeenkomst. Indien geen opzegtermijn in de Overeenkomst is opgenomen, kan de Stadsbank de Overeenkomst opzeggen met inachtneming van een redelijke opzegtermijn, mede gelet op de duur van de Overeenkomst.

Artikel 25 Ontbinding

25.1. Ieder der Partijen heeft het recht de Overeenkomst zonder rechterlijke tussenkomst en zonder ingebrekestelling met onmiddellijke ingang te ontbinden, indien:

- artikel 4.4 algemene inkoopvoorwaarden wordt geschonden;
- de andere Partij een besluit tot ontbinding van de rechtspersoon of onderneming heeft genomen;
- de zeggenschap van de andere Partij bij een ander komt te rusten dan ten tijde van het sluiten van deze Overeenkomst;
- ten aanzien van de andere Partij faillissement is aangevraagd dan wel uitgesproken of, al dan niet voorlopig, surséance van betaling is aangevraagd of verleend;
- de andere Partij fuseert, splitst of op enigerlei wijze (een deel van) zijn bedrijf overdraagt;
- de andere Partij in een situatie van overmacht verkeert gedurende meer dan tien dagen.

25.2. Elke ontbinding als bedoeld in lid 1 dient terstond door middel van een aangetekend schrijven te geschieden.

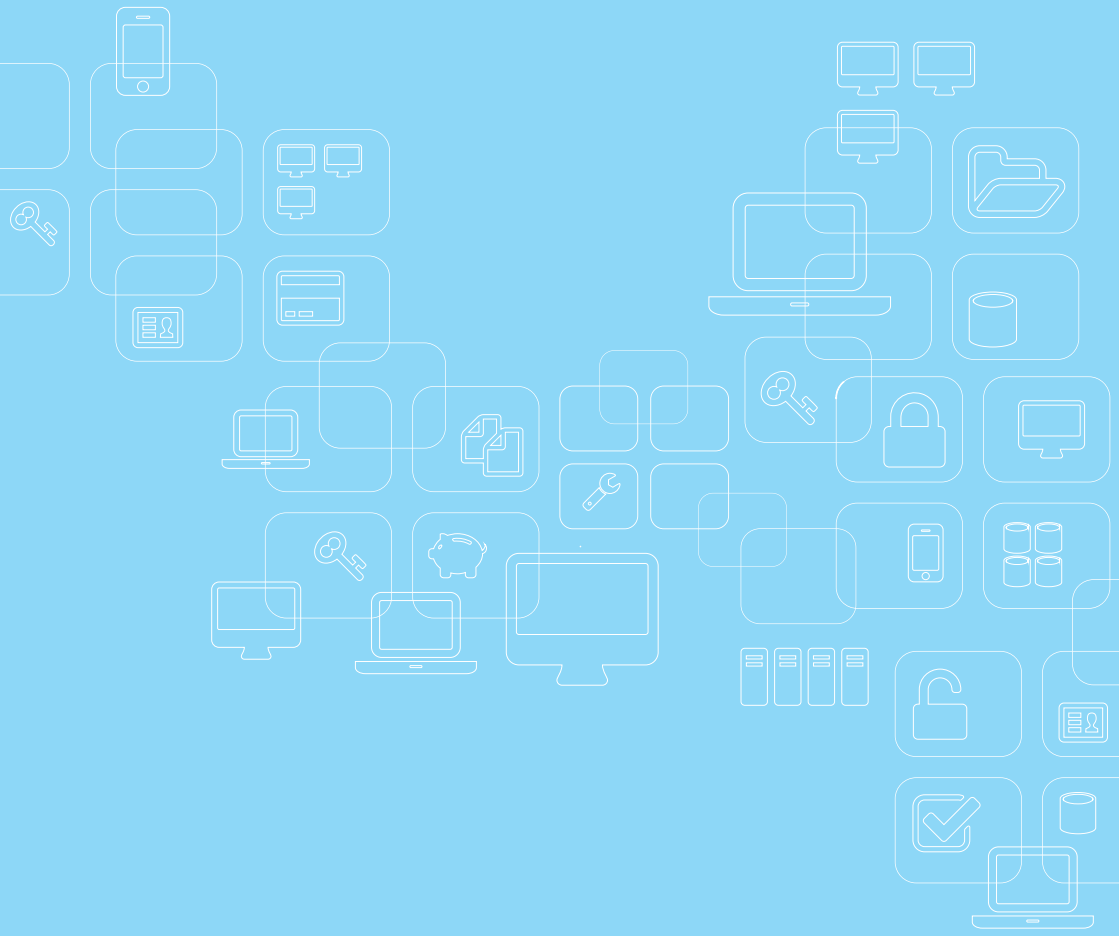
25.3. Ingeval van ontbinding door de Stadsbank als bedoeld in lid 1 is de Stadsbank geen vergoeding verschuldigd aan de Contractant voor de Prestaties die niet door Contractant zijn verricht. Eventuele aan de Contractant verrichte onverschuldigde betalingen, betaalt de Contractant terug aan de Stadsbank, vermeerderd met wettelijke rente vanaf de dag waarop dit is betaald.

Artikel 26 Vernietiging

26.1. Indien één van de Partijen zich beroept op vernietiging door middel van een buitengerechtelijke verklaring, dient dit te geschieden met een aangetekend schrijven.

KWALITEITS INSTITUUT NEDERLANDSE GEMEENTEN

GIBIT Gemeentelijke Inkoopvoorwaarden bij IT



GIBIT Gemeentelijke Inkoopvoorwaarden bij IT

Inhoudsopgave

Voorwoord

GIBIT is een grote aanwinst

De totstandkoming van de GIBIT (Gemeentelijke Inkoopvoorwaarden bij IT) is onderdeel van het programma Digitale Agenda 2020. Een van de speerpunten van die Digitale Agenda 2020 is het professionaliseren van het ICT-opdrachtgeverschap bij gemeenten om hiermee te borgen dat gemeenten ICT-producten en –diensten kopen die aansluiten bij hun behoeften.

Als u of ik een schildersbedrijf inhuren, dan weten we vaak precies wat we kunnen verwachten en tegen welke prijs. Als gemeenten ICT-producten of diensten aanschaffen, dan is er vaak nog onvoldoende grip op wat ze krijgen (een systeem dat werkt in samenhang met andere ICT-producten) en wat ze betalen (prijsverhogingen, wat wel/niet in onderhoud en ondersteuning is meegenomen, etc.). Bij gebruik van de GIBIT hebben gemeenten meer waarborgen dat ze een product krijgen dat past bij wat ze echt willen en waarvoor duidelijke afspraken zijn gemaakt.

Tegelijkertijd is de GIBIT niet eenzijdig. Goed opdrachtgeverschap vraagt ook om afstemming met leveranciers over producten en

diensten waar die partijen aan kunnen voldoen. Dat vraagt om wederzijds vertrouwen en evenwichtige voorwaarden.

In het afgelopen jaar is de GIBIT tot stand gekomen met behulp van een groot aantal partijen. Juristen, inkopers, informatiemanagers, maar ook leveranciers. Ik wil graag een groot compliment maken aan al die partijen die hebben meegedacht over en meegewerkt aan een product dat zeker gezien mag worden als grote aanwinst en ik beveel alle gemeenten aan om de GIBIT te gebruiken.

Arjen Gerritsen is burgemeester van Almelo en lid van de VNG-commissie Dienstverlening & Informatiebeleid. Als ambassadeur was hij betrokken bij de totstandkoming van de GIBIT.

Inleiding

Gemeenten krijgen met GIBIT eigen inkoopvoorwaarden

Gemeenten zetten vol in op digitalisering, waarbij bedrijfsprocessen soms volledig worden geautomatiseerd. Dit betekent dat gemeenten voor de kwaliteit van hun dienstverlening en uitvoering steeds meer afhankelijk zijn van de kwaliteit van ingekochte ICT-producten en –diensten. Deze producten en diensten worden geleverd door bijna tweehonderd leveranciers. Gemeenschappelijke ICT-inkoopvoorwaarden, specifiek voor gemeenten, zijn uiterst nuttig om de kwaliteit van de producten en diensten goed aan te laten sluiten op de gemeentelijke behoeften en doelstellingen.

Om het ICT-opdrachtgeverschap verder te professionaliseren en de ICT-inkoopvoorwaarden te uniformeren, heeft KING in 2015 onder gemeenten een verkenning uitgevoerd. Daaruit kwam naar voren dat gemeenten in ketens willen kunnen werken en informatie veilig en betrouwbaar willen kunnen uitwisselen. Tegelijkertijd gaan gemeenten steeds meer samenwerken, ICT-zaken meer collectief organiseren en innovaties benutten. Dat betekent behoefte aan meer flexibiliteit van hun informatievoorziening.

Dat heeft ook zijn weerslag op de voorwaarden die worden gesteld aan ICT-producten en -diensten die uit de markt worden betrokken. Het betekent bijvoorbeeld meer flexibiliteit in licenties, meer aandacht voor data-overdracht en het gemakkelijker kunnen vervangen van systemen. Ook compliancy (het aantoonbaar voldoen aan bestaande normen en standaarden en architectuur), aansluiting op de generieke digitale infrastructuur van de overheid (GDI), cloud- en hostingservices en informatiebeveiliging en privacy waren onderwerpen die veelvuldig werden genoemd.

Afgelopen jaar is binnen het programma Digitale Agenda 2020 door KING de GIBIT (Gemeentelijke Inkoopvoorwaarden bij IT) gerealiseerd. Bij het opstellen van de GIBIT is een grote en gevarieerde groep betrokken geweest: juristen, inkopers en informatiemanagers vanuit gemeenten en verder experts vanuit KING, juridische specialisten, de Informatiebeveiligingsdienst voor gemeenten (IBD), de VNG Adviescommissie Archieven en een vertegenwoordiging van leveranciers binnen de klankbordgroep.

Vanuit de VNG Commissie Dienstverlening en Informatiebeleid is Arjen Gerritsen, voormalig burgemeester van De Bilt en sinds eind september eerste burger van Almelo, als ambassadeur betrokken. Ook leveranciers waren bij het opstellen van de GIBIT betrokken. Ook al omdat met de GIBIT ernaar wordt gestreefd dat het niet alleen gebruikt wordt als kader voor de inkoop, maar óók breed wordt geaccepteerd door leveranciers.

Larissa Zegveld, directeur van KING, vindt dat de GIBIT goed past in een beeld waarbij gemeenten (én leveranciers) steeds vaker de samenwerking opzoeken. ‘Veel activiteiten in de

uitvoering bij gemeenten lijken op elkaar. Gemeenten zoeken naar oplossingen om dit werk effectiever en efficiënter te doen, met minder mensen en met de inzet van technologie. Zij kijken daarbij naar collectivisering. Ofwel, ze gaan meer samenwerken. Dat geeft beweging in de markt en zal leiden tot een ander samenspel van overheid en markt. Een samenspel dat veel meer over partnerschap zal gaan. De overheid ziet zich gesteld voor forse uitdagingen en heeft het innovatieve vermogen van de markt nodig om hier de meest optimale antwoorden op te vinden. Dat moeten we samen verkennen en onderzoeken.'

Het realiseren van de GIBIT is in nauwe samenwerking met gemeenten en leveranciers gedaan. Zegveld: 'Ik ben heel tevreden over de bijdrage van juristen, inkopers en I&A-deskundigen in de werkgroep van gemeenten. Ook de leden in de klankbordgroep van leveranciers hebben waardevolle inbreng geleverd. Voor zover deze inbreng passend en redelijk was, en het belang van gemeenten niet in het geding was, is deze gehonoreerd en in de GIBIT opgenomen. Ik ben erg ingenomen met het resultaat en wil alle deelnemers dan ook graag hartelijk bedanken voor hun bijdrage aan de GIBIT.'

KING is de partij die gemeenten bij de collectivisering (in de informatievoorziening) ondersteunt. Zegveld: 'Sinds onze oprichting in 2009 hebben wij daarvoor een heel palet aan diensten ontwikkeld. Dat palet, die kast als het ware, wordt steeds beter gevuld met allerlei standaarden en diensten die gemeenten kunnen gebruiken. Zoals de GIBIT. Om de beoogde effecten te bereiken, is het noodzakelijk dat dit palet ook

daadwerkelijk wordt gebruikt. In dat kader is een implementatieondersteuning gepland.

Concreet betekent dit het beschikbaar stellen van hulpmiddelen voor inkoop. Zoals hostingovereenkomsten, aankoop van software of het aanmaken of aanpassen van bewerkersovereenkomsten, waarin GIBIT al direct verweven zit. Verder is er een traject waarbij inkopers/juristen van gemeenten breed worden geïnformeerd over de inhoud en het toepassen van de GIBIT.'

I Totstandkoming GIBIT

Achtergrond en terugblik

In samenwerking met gemeenten heeft KING in het voorjaar van 2015 een verkenning uitgevoerd naar verbetering en uniformering van ICT-inkoopvoorwaarden van gemeenten. Meer dan 100 gemeenten en gemeentelijke samenwerkingsverbanden hebben bijgedragen aan de verkenning en het advies voor het vervolgtraject (zie www.gibit.nl voor de rapportage). Uit de verkenning komt naar voren dat de behoefte aan betere en uniforme inkoopvoorwaarden onder gemeenten groot is. Het past in de lijn van beter opdrachtgeverschap. Passende ICT-inkoopvoorwaarden zijn voor gemeenten een belangrijke randvoorwaarde bij het verbeteren en vernieuwen van de digitale informatievoorziening en om flexibiliteit te krijgen. Dit sluit aan bij de ambitie van de Digitale Agenda 2020 om te werken als één overheid en het opdrachtgeverschap te professionaliseren.

Vanuit de verkenning is geadviseerd om de ARBIT als basis te gebruiken voor de gemeentelijke inkoopvoorwaarden. Specifieke zaken die binnen het gemeentelijk domein relevant zijn, dienen toegevoegd te worden, zoals: bepalingen omtrent flexibiliteit

(onder meer bij samenwerkingen en migraties), het (aantoonbare) gebruik van standaarden (onder meer gemeente specifieke standaarden), veiligheid (onder meer informatiebeveiliging en privacy) en aansluiten op Cloud-ontwikkelingen en landelijke infrastructuur. Daarnaast is gevraagd om met – voor zover mogelijk – evenwichtige voorwaarden te komen om (terugkomende) discussies tijdens contractering te beperken. Tot slot zijn naast voorwaarden ook sjablonen en hulpmiddelen nodig voor het gebruik.

Op de Algemene Ledenvergadering van de VNG in juni 2015 is besloten invulling te geven aan de uitgevoerde verkenning en het advies. Dit heeft geresulteerd in de voorliggende Gemeentelijke Inkoopvoorwaarden bij IT (GIBIT).

Gevolgde aanpak opstellen GIBIT

Bij het opstellen van de GIBIT is de volgende projectstructuur gevolgd:

- Bestuurlijke ambassadeur vanuit de VNG Commissie Dienstverlening en Informatiebeleid (Arjen Gerritsen, voormalig burgemeester gemeente De Bilt, momenteel Almelo);
- Projectleiding en advies vanuit KING;
- Werkgroep van gemeenten en gemeentelijke samenwerkingsverbanden, bestaande uit de gemeenten Apeldoorn, Assen, Barneveld, Berkelland, De Bilt, Delft, Ede, Haarlem, Hilversum, Kerkrade, Langedijk, Oegstgeest, Purmerend, Wijchen, Westland en tevens vertegenwoordiging van de VIAG, GV Centric en GV PinkRoccade. De deelname is evenredig verspreid over juristen, inkopers en informatiemanagers;
- Klankbordgroep van leveranciers, bestaande uit BCT, Centric, Decos, Infosupport, KPN, Metaobjects, PinkRoccade, RAET, SIMgroep, Topicus en Solipsis;

- Penvoerder GIBIT door Dirkzwager advocaten & notarissen;
- Inhoudelijke ondersteuning en ontwikkelen hulpmiddelen (waaronder modelovereenkomsten) door ICTRecht;
- Inhoudelijke ondersteuning vanuit de Informatiebeveiligingsdienst voor gemeenten (IBD);
- Inhoudelijke afstemming met de VNG Adviescommissie Archieven;
- 204 volgers vanuit gemeenten, welke op de hoogte worden gehouden van tussenresultaten;
- 32 volgers vanuit leveranciers, welke op de hoogte worden gehouden van tussenresultaten.

Binnen de gemeentelijke werkgroep zijn de keuzes gemaakt welke bepalingen op welke wijze zijn opgenomen. Er zijn bijeenkomsten met de klankbordgroep van leveranciers geweest waar de leveranciers reacties en suggesties op conceptversies van de GIBIT hebben kunnen geven. Aan de gemeenten is vervolgens de keus gelaten dit over te nemen of niet. Voor zover de gemeenten de suggesties passend en evenwichtig vonden, zijn ze overgenomen. Deze werkwijze is ook gevolgd bij de reacties die tijdens de brede consultatie zijn gegeven. Aan deze brede consultatie hebben 95 organisaties deelgenomen. De uitkomsten daarvan inclusief de (voorgestelde) wijzigingen naar aanleiding van de consultatie zijn meerdere malen besproken met de klankbordgroep van leveranciers en binnen de werkgroep van gemeenten.

Door deze werkwijze te volgen menen we evenwichtigere voorwaarden te hebben opgesteld dan die in het verleden vaak gebruikt werden. Niet in alle gevallen is volledige overeenstemming bereikt ten aanzien van de wensen van leveranciers. We zijn ons

bewust dat in voorkomende gevallen het belang van de gemeenten zwaarder heeft geteld dan het meegaan met alle suggesties vanuit leveranciers.

Vaststelling

Binnen de gemeentelijke werkgroep is tot de definitieve inhoud en versie van de GIBIT besloten. In september 2016 heeft de Commissie Dienstverlening en Informatiebeleid positief geadviseerd over de vaststelling van de GIBIT. Op 8 december 2016 heeft de VNG de GIBIT vastgesteld.

Implementatie en hulpmiddelen

Na vaststelling volgt implementatie van de GIBIT. Hiertoe worden gemeenten door KING ondersteund in het toepassen van de GIBIT. Enerzijds wordt dit gedaan door kennissessies te organiseren waar de GIBIT wordt toegelicht. Anderzijds wordt dit gedaan door hulpmiddelen ter beschikking te stellen. Een voorbeeld hiervan is een online contractgenerator die gemeenten binnen hun inkoopproces ondersteunt. Hiermee kunnen efficiënt toegesneden overeenkomsten worden opgesteld waarbij rekening kan worden gehouden wordt met de zwaarte van het bedrijfsbelang en de aard van de in te kopen ICT Prestatie.

KING verzorgt deze implementatieondersteuning en biedt deze hulpmiddelen aan als activiteit binnen de Digitale Agenda 2020. Tevens is reeds besloten dat het beheer van de GIBIT inclusief de hulpmiddelen vanuit dit programma geborgd zijn. Onderdeel van het beheer is de evaluatie van het gebruik van de GIBIT wat mogelijk tot aanscherping/bijstelling van de GIBIT kan leiden. Tevens worden de bij de GIBIT behorende Gemeentelijke ICT-kwa-

liteitsnormen bijgehouden. Dit laatste zal een hogere dynamiek kennen dan de GIBIT zelf. Kijk voor de meest actuele versie altijd op www.gibit.nl. Advies is daar altijd te kijken voor gebruik van de GIBIT en/of hulpmiddelen.

II Inhoudelijke toelichting – algemeen

Reikwijdte van GIBIT

De GIBIT betreft Gemeentelijke Inkoopvoorwaarden bij IT.
De reikwijdte omvat primair alle producten en/of diensten die gemeenten en gemeentelijke samenwerkingsverbanden op het gebied van ICT verwerven. Dit betreft onder meer, doch niet uitsluitend:

- **Producten:** (onderdelen van) standaard en maatwerk software, systeemsoftware, databases, hardware en/of (complete) IT-systemen, een en ander met bijbehorende materialen, koppelingen, toegang tot opgeslagen gegevens, hulpmiddelen, vervangingsonderdelen en documentatie, het verstrekken van softwarelicenties en/of intellectuele eigendomsrechten;
- **Diensten van projectmatige aard:** het leveren, converteren, installeren, inrichten, koppelen, implementeren, onderhouden, ontvlechten, repareren en vervaardigen van en adviseren over ICT-zaken en/of diensten, inclusief het verzorgen van opleidingen/trainingen;
- **Diensten van structurele aard:** het onderhouden, op afstand aanbieden en/of 'hosten' van software(applicaties), clouddiensten, netwerken en websites, het (laten) registreren

van domeinnamen, het ontwerpen en ontsluiten van websites en webtoepassingen, het bijhouden en ontsluiten van content en support en incidentmanagement.

In het vervolg van het document wordt daar waar 'gemeenten' staat ook bedoeld gemeentelijke samenwerkingsverbanden of andere (al dan niet aan de gemeente gelieerde) instanties die gebruik maken van de GIBIT.

Naast het primaire toepassingsgebied zijn verschillende delen uit de GIBIT ook goed toepasbaar voor allerlei andere gemeentelijke inkooptrajecten. Er zit immers in steeds meer zaken een ICT-component die data registreert, verwerkt en/of communiceert. Een voorbeeld is het Internet of Things waarbij in afvalcontainers, bruggen, lantaarnpalen, vervoersmiddelen, verkeerssystemen, camera's, meet- en signaleringsysteem en allerlei andere zaken in de publieke ruimte steeds vaker een ICT-component is opgenomen.

Hoewel de GIBIT primair bedoeld is voor inkoop van ICT-producten en diensten kunnen delen van de GIBIT worden gebruikt voor een betere borging van informatiebeveiliging, eigendom en overdracht van data en (data)interoperabiliteit voor zaken welke ook een ICT-component hebben.

GIBIT en aanbestedingswet/regelgeving en EU-richtlijnen

De GIBIT is bruikbaar voor actuele wet- en regelgeving voor aanbestedingen. De nieuwe aanbestedingsregelgeving is het gevolg van de implementatie van de aanbestedingsrichtlijnen 2014/23, 2014/24 en 2014/25 die in 2014 door het Europees Parlement

zijn aangenomen. In deze richtlijnen worden nagenoeg uitsluitend regels gesteld voor het verloop en de inhoud van de aanbestedingsprocedure en dus niet voor de contractvoorwaarden. De richtlijnen regelen daarmee niet de voorwaarden in de Nederlandse aanbestedingsregelgeving, waaronder de Gids Proportionaliteit en de inhoud van de overeenkomst zoals de risicoverdeling en de beperking van aansprakelijkheid. Die onderwerpen zijn niet gewijzigd.

Wij wijzen er nadrukkelijk op dat de gemeenten steeds per project zullen moeten afwegen in hoeverre bepaalde afspraken proportioneel zijn. Bij het opstellen van de GIBIT is getracht met een veelheid aan situaties rekening te houden. Wij verwachten dan ook dat de GIBIT in de regel zal voldoen aan de eisen van proportionaliteit. Dat laat de eigen verantwoordelijkheid van de gebruikers van de GIBIT, om hier per situatie naar te kijken, uiteraard onverlet.

Juridisch inkoopkader met abstract karakter

De GIBIT is bedoeld als algemeen juridisch inkoopkader voor een veelheid aan verschillende ICT-producten/diensten. Dit maakt dat diverse bepalingen noodzakelijkerwijs abstract van karakter zijn. De GIBIT heeft daarnaast diverse vangnetbepalingen. Indien in een overeenkomst met een leverancier geen specifieke afspraken worden gemaakt en de GIBIT is van toepassing verklaard, dan gelden de vangnetbepalingen zoals opgenomen in de GIBIT. Indien in de overeenkomst ten opzichte van de vangnetbepalingen afwijkende afspraken zijn gemaakt, dan gaan die uiteraard voor. Hetzelfde principe gaat op voor de wet: daar waar in de GIBIT of de Overeenkomst geen van het wettelijk systeem afwijkende keuzes zijn gemaakt, geldt het normale wettelijke systeem onverkort.

Opbouw GIBIT via Life Cycle van ICT-producten

De GIBIT is opgezet om de complete 'life cycle' van een te gebruiken ICT-product/dienst te ondersteunen. Alle fasen van een ICT-product/dienst komen dan ook in de voorwaarden naar voren, zowel de eenmalige projectmatige werkzaamheden (zoals implementatie) als de meer structurele activiteiten (zoals hosting services). Ook staan er exit voorwaarden in. Dus vanaf de selectie via eventuele ontwikkeling naar implementatie, acceptatie, gebruik, support, onderhoud en uiteindelijk de uitfasering, overstap en exit.

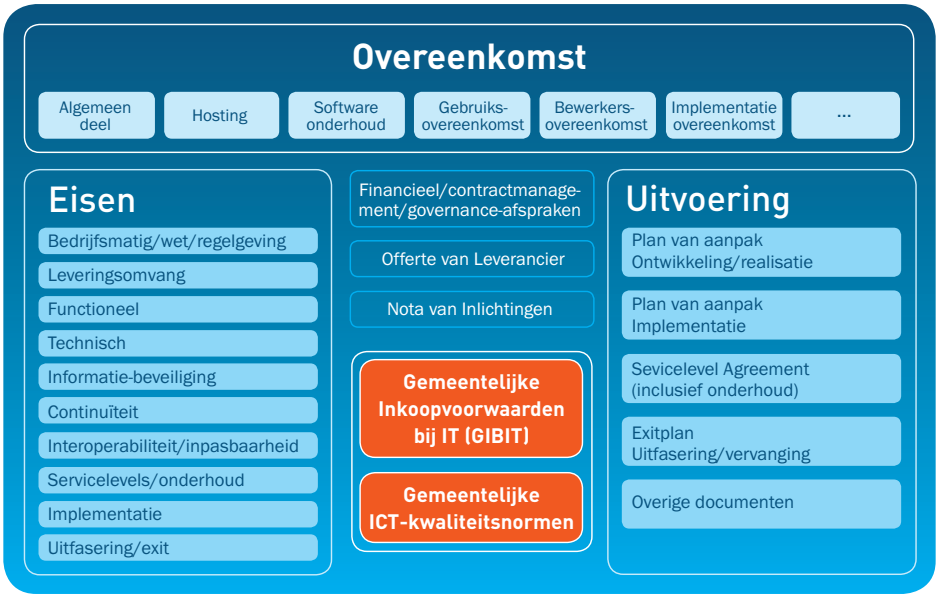
Voor al die fasen geldt dat in de GIBIT bepaalde keuzes zijn gemaakt. In die keuzes is bewust niet steeds alleen het (eenzijdige) belang van de opdrachtgever in ogenschouw genomen, maar is gepoogd het redelijke midden te zoeken. Uiteraard zonder afbreuk te doen aan het belang van de gemeente.

Tenslotte zet de GIBIT partijen er in (bijna) al die fasen toe aan om bepaalde aspecten/onderwerpen nader uit te werken en bepaalde risico's uitdrukkelijk te onderkennen en te adresseren. Door risico's vroegtijdig te signaleren, kunnen partijen in alle redelijkheid daarover het gesprek aangaan, in plaats van achteraf te moeten belanden in (complexe) discussies over meerwerk, tekortkomingen en niet uitgekomen verwachtingen.

GIBIT binnen modulaire voorwaarden- en overeenkomstenstructuur

De GIBIT staat niet op zichzelf. De GIBIT maakt deel uit van een samenhangend en modulair opgezette voorwaarden- en overeenkomstenstructuur waarin afspraken voor een ICT-product/dienst

zijn opgenomen. De structuur – en daarbinnen de positie van de GIBIT – is schematisch in onderstaande figuur weergegeven.



In de (bovenliggende) overeenkomst, of deelovereenkomsten, tussen opdrachtgever en leverancier wordt bepaald WAT er aan product(en) en/of dienst(en) wordt afgenomen en welke specifieke afspraken gemaakt worden. Hierbij kan in bovenliggende overeenkomsten worden afgeweken van bepaalde (vangnet) bepalingen in de GIBIT.

De overeenkomst prevaleert dan ook op het bepaalde in de GIBIT. Als in de overeenkomst geen andere keuzes zijn gemaakt of bepaalde aspecten niet zijn meegenomen, dan functioneert de GIBIT als vangnet. Belangrijk is om de GIBIT dan ook al vanaf de offerteaanvraag van toepassing te verklaren.

Naast de overeenkomst(en) en de GIBIT geldt dat een diversiteit aan andere documenten deel kunnen uitmaken van het totaal aan afspraken. Dit betreft onder meer de uitwerkingen van wensen en eisen (bijvoorbeeld een programma van eisen, al dan niet functioneel beschreven), financiële en contractuele afspraken, offertes, nota's van inlichtingen, service level agreements, implementatieplan etc..

De Gemeentelijke ICT-kwaliteitsnormen behoren bij de GIBIT. Deze normen zijn op www.gibit.nl gespecificeerd, inclusief het werkingsgebied van die normen. Voorbeelden van normen zijn bijvoorbeeld de StUF-standaarden en/of koppelvlakstandaarden die van toepassing zijn. Indien voor het werkingsgebied van de gevraagde ICT Prestatie bepaalde normen van toepassing zijn, dan zijn deze normen opgenomen als onderdeel van de Gemeentelijke ICT-kwaliteitsnormen, zoals gepubliceerd op www.gibit.nl en is daarmee in de GIBIT opgenomen dat aan deze normen voldaan moet worden. Bij gebruik van de GIBIT verplicht een leverancier zich dan ook aan deze normen te houden. Dit betreft de normen zoals vastgesteld ten tijde van het sluiten van de overeenkomst. De GIBIT gaat er standaard van uit dat de leverancier ook gedurende de looptijd van de overeenkomst moet blijven voldoen aan – eventueel bijgestelde – normen.

Op www.gibit.nl staat de meest actuele versie van de GIBIT inclusief handreikingen en hulpmiddelen voor toepassing van de GIBIT tijdens het inkoopproces. Advies is om altijd daar te kijken voor de meest actuele versie. Qua beheer worden de Gemeentelijke ICT-kwaliteitseisen naar verwachting vaker aangepast dan de GIBIT zelf. Elke aanpassing wordt duidelijk zichtbaar gemaakt.

III Gemeentelijke inkoopvoorwaarden bij IT (GIBIT) INDEX

I. Algemeen deel

II. Privacy, beveiliging en archivering

III. Hosting

III Gemeentelijke inkoopvoorwaarden bij IT (GIBIT) Versie 2016

I. Algemeen deel

Artikel 1. Begrippen

In deze Gemeentelijke Inkoopvoorwaarden bij IT (GIBIT) worden de navolgende begrippen met een (begin)hoofdletter gebruikt:

1.1 **Acceptatie:** De formele goedkeuring van (onderdelen van) de ICT Prestatie, afzonderlijk en in samenhang met elkaar, door middel van een succesvol uitgevoerde (integrale) Acceptatieprocedure.

1.2 **Acceptatieprocedure:** De testprocedure waarmee kan worden aangetoond dat de ICT Prestatie geen Gebrek(en) bevat.

1.3 **Applicatielandschap:** het geheel van interne en externe systemen, software, databanken, koppelingen, apparatuur, ICT-infrastructuur en hulpmiddelen die voor de Opdrachtgever de geautomatiseerde informatievoorziening vormt waarbinnen de ICT Prestatie ingepast wordt.

1.4 **Beschikbaarheid:** de mate waarin de ICT Prestatie daadwerkelijk beschikbaar is voor Opdrachtgever en gebruikt kan worden.

1.5 **Conversie:** Het converteren en migreren van gegevensbestanden van Opdrachtgever van het oude systeem naar de nieuwe ICT Prestatie, zonder daarbij de volledigheid, de integriteit en de metadata van de gegevens aan te tasten.

1.6 **Correctief Onderhoud:** het opsporen en herstellen door Leverancier van Gebreken die Opdrachtgever hem heeft gemeld of die Leverancier anderszins bekend zijn geworden.

1.7 **Derdenprogrammatuur:** Programmatuur waarvan (a) de intellectuele eigendomsrechten geheel niet bij Leverancier en/of een aan Leverancier gelieerde vennootschap rusten en (b) waarbij Leverancier niet in staat is bepaalde ontwikkelingen aan / wijzigingen in die programmatuur af te dwingen.

1.8 **Functiehersteltijd:** de periode gelegen tussen het moment waarop een Gebrek bij Leverancier wordt gemeld en het moment waarop dit is verholpen.

1.9 **Gebrek:** Een storing of het niet of niet volledig voldoen van de ICT Prestatie aan het Overeengekomen gebruik.

1.10 **Gebruiksrecht:** het recht op grond waarvan Opdrachtgever bevoegd is tot het gebruik van de ICT Prestatie.

1.11 **Gemeentelijke ICT-kwaliteitsnormen:** de door Kwaliteitsinstituut Nederlandse Gemeenten (KING) en Vereniging Nederlandse Gemeenten (VNG) op www.gibit.nl gepubliceerde en van tijd tot tijd bijgewerkte normen en standaarden voor ICT-producten en diensten.

1.12 **GIBIT:** de onderhavige Gemeentelijke inkoopvoorwaarden bij IT, zoals vastgesteld door de VNG d.d. 8 december 2016.

1.13 **Hosting:** het door Leverancier door middel van technieken voor communicatie op afstand aan Opdrachtgever ter beschikking stellen van de ICT Prestatie.

1.14 **ICT Prestatie:** alle door Leverancier op grond van de Overeenkomst te leveren goederen (waaronder begrepen Gebruiksrechten) en diensten.

1.15 **Implementatie:** Het geheel van handelingen en activiteiten dat nodig is om alle onderdelen van de ICT Prestatie, afzonderlijk en in onderlinge samenhang, in gebruik te kunnen nemen in de organisatie van Opdrachtgever, zodanig dat alle gebruikers van Opdrachtgever ermee kunnen werken overeenkomstig het Overeengekomen gebruik. Tot de Implementatie behoort tevens de Conversie, het realiseren van de voor het Overeengekomen gebruik noodzakelijke Koppelingen en het uitvoeren van de Acceptatieprocedure.

1.16 **Implementatieplan:** Het plan van aanpak voor de Implementatie, waarin een concrete uitwerking is opgenomen van de door de betrokken partijen in dit kader te verrichten activiteiten, de te implementeren en/of te ontwikkelen ICT Prestatie, de verantwoordelijkheden van Leverancier en Opdrachtgever en de tijdsplanning.

1.17 **Innovatief Onderhoud:** het beschikbaar stellen door Leverancier aan Opdrachtgever van Updates en/of Upgrades van de ICT Prestatie.

1.18 **Interoperabiliteitseisen:** de in de Overeenkomst opgenomen eisen die aan de ICT Prestatie worden gesteld om gegevens uit te kunnen wisselen met of anderszins samen te kunnen werken met andere onderdelen van het Applicatielandschap.

1.19 **Koppeling:** de systematiek voor uitwisseling van gegevens tussen enerzijds de ICT Prestatie en anderzijds (onderdelen van) het Applicatielandschap.

1.20 **Leverancier:** de partij waarmee Opdrachtgever een Overeenkomst gesloten heeft.

1.21 **Onderhoud:** het geheel van Correctief Onderhoud, Preventief Onderhoud, Innovatief Onderhoud en gebruikersondersteuning, een en ander zoals nader uitgewerkt in de GIBIT, de Overeenkomst en de SLA.

1.22 **Opdrachtgever:** de partij ten behoeve waarvan de Overeenkomst wordt gesloten.

1.23 **Overeengekomen gebruik:** het door Opdrachtgever beoogde gebruik van de ICT Prestatie zoals dat ten tijde van het sluiten van de Overeenkomst voor Leverancier (al dan niet op basis van de offerteaanvraag of andere aan de Overeenkomst voorafgaande documenten) bekend was of op grond van artikel 3 voor Leverancier bekend behoorde te zijn, een en ander voor zover dat gebruik in de Overeenkomst niet uitdrukkelijk is uitgesloten of beperkt.

1.24 **Overeenkomst:** de afspraken tussen Opdrachtgever en Leverancier met betrekking tot de levering van de ICT Prestatie, waarvan de GIBIT onderdeel uitmaakt. Overeenkomsten die worden gesloten onder een mantel- of raamovereenkomst worden voor deze voorwaarden steeds als afzonderlijke Overeenkomst beschouwd.

1.25 **Personeel:** de door partijen bij de uitvoering van de Overeenkomst in te schakelen personeelsleden en/of hulppersonen.

1.26 **Preventief Onderhoud:** het treffen van maatregelen door Leverancier ter voorkoming van Gebreken en andere technische problemen en andere daarmee verband houdende vormen van dienstverlening.

1.27 **Programmatuur:** het geheel van de door Leverancier te leveren programmatuur (software).

1.28 **Reactietijd:** de tijd waarbinnen Leverancier op een melding door Opdrachtgever van een Gebrek en andere verzoeken van Opdrachtgever om dienstverlening, adequaat moet reageren.

1.29 **Service levels:** ten aanzien van Onderhoud en andere overeengekomen vormen van dienstverlening in de Overeenkomst opgenomen eisen en prestatienormen zoals Reactie- en Functiehersteltijden.

1.30 **Update(s):** een opvolgende versie van de ICT Prestatie waarin Gebreken zijn hersteld en/of de werking van de ICT Prestatie anderszins is verbeterd.

1.31 **Upgrade(s):** een opvolgende versie van de ICT Prestatie met in overwegende mate nieuwe of gewijzigde functionaliteiten, al dan niet onder een andere naam uitgebracht.

1.32 **Vergoeding:** de in totaal voor de ICT Prestatie overeengekomen prijs, te berekenen op basis van de initieel beoogde looptijd van de Overeenkomst en inclusief de initiële begroting van de werkzaamheden waarvoor geen vaste prijs is overeengekomen (alles ex. BTW).

Artikel 2. Toepasselijkheid

2.1 De GIBIT is van toepassing op en maakt deel uit van alle aanvragen, offertes, aanbiedingen, opdrachtbevestigingen, bestellingen, overeenkomsten en alle andere rechtshandelingen tussen Opdrachtgever en Leverancier die betrekking hebben op de in de Overeenkomst gespecificeerde en daarmee samenhangende ICT Prestatie.

2.2 De GIBIT bestaat uit drie hoofdstukken:

i) hoofdstuk I (dat altijd van toepassing is); en

ii) hoofdstuk II inzake privacy, beveiliging en archiefbeheer (dat van toepassing is indien met de ICT Prestatie gegevens van Opdrachtgever worden verwerkt); en

iii) hoofdstuk III inzake Hosting (dat van toepassing is bij het verlenen van Hosting).

2.3 De toepasselijkheid van enige algemene of specifieke voorwaarden of bedingen van Leverancier, onder welke benaming ook, wordt uitdrukkelijk van de hand gewezen.

2.4 Mocht enige bepaling van de GIBIT nietig zijn of vernietigd worden, of mocht enige bepaling van de GIBIT naar het oordeel van de rechter niet van toepassing of ongeldig zijn, dan zal slechts de betreffende

bepaling als niet geschreven worden beschouwd, maar zullen de GIBIT voor het overige volledig van kracht blijven. Partijen zullen in overleg treden om de betreffende niet toepasselijke of ongeldige bepaling te vervangen door een nieuwe bepaling, waarbij zoveel mogelijk het doel en de strekking van de eerdere bepaling in acht zal worden genomen.

2.5 In geval van strijdigheid tussen het bepaalde in de GIBIT en het bepaalde in de Overeenkomst prevaleert het bepaalde in de Overeenkomst boven het bepaalde in de GIBIT.

2.6 Wijzigingen van en aanvullingen op de GIBIT gelden slechts indien deze schriftelijk tussen partijen zijn overeengekomen. De wijziging en/of aanvulling geldt slechts voor de in artikel 2.1 bedoelde Overeenkomst.

Artikel 3. Totstandkoming overeenkomst

3.1 Een aanvraag voor een offerte of een andere uitnodiging tot het doen van een aanbod bindt Opdrachtgever niet. Offertes zijn kosteloos en hebben een geldigheidsduur van minimaal 90 dagen.

3.2 Alvorens een aanbod aan Opdrachtgever te doen heeft Leverancier zich in voldoende mate op de hoogte gesteld van:

i) de doelstellingen, in verband waarmee Opdrachtgever de Overeenkomst wil aangaan;

ii) de organisatie en het Applicatielandschap van Opdrachtgever, voor zover van belang voor de Overeenkomst.

3.3 Indien en voor zover Leverancier beschikt over onvoldoende informatie om aan de in het vorige lid bedoelde verplichting te voldoen, dient zij hieromtrent navraag te doen bij Opdrachtgever. Opdrachtgever zal alle in redelijkheid verlangde informatie aan Leverancier verstrekken (tenzij deze vertrouwelijk van aard is en in redelijkheid ook niet onder een geheimhoudingsovereenkomst verstrekt kan worden).

3.4 Leverancier houdt bij het doen van een aanbod tot het verrichten van de ICT Prestatie rekening met de in de vorige twee leden bedoelde informatie.

3.5 Leverancier dient, tenzij anders overeengekomen en onverminderd het bepaalde in artikel 4.2, voorafgaand aan de totstandkoming van de Overeenkomst een risicoanalyse uit te voeren met betrekking tot de door Opdrachtgever beoogde ICT Prestatie. Deze risicoanalyse is met name gebaseerd op de in de leden 2 en 3 bedoelde informatie.

Leverancier dient de eventueel gesignaleerde risico's en de in dat kader benodigde beheersmaatregelen te adresseren in het aanbod aan Opdrachtgever.

3.6 In geval van een aanbesteding in de zin van de Aanbestedingswet worden de in de leden 2 t/m 5 bedoelde verplichtingen begrensd door de inhoud, aard en omvang van de in de aanbestedingsdocumenten verstrekte informatie.

3.7 Indien de ICT Prestatie (deels) de levering van Derdenprogrammatuur behelst, of van Derdenprogrammatuur afhankelijk is, geldt tevens het bepaalde in artikel 19.

3.8 Een overeenkomst komt eerst tot stand nadat hetzij (1) Opdrachtgever een schriftelijk aanbod van Leverancier schriftelijk heeft aanvaard, (2) partijen een schriftelijk opgemaakte overeenkomst hebben ondertekend of (3) Leverancier uitvoering geeft aan een schriftelijke opdracht van Opdrachtgever.

Artikel 4. Uitvoering van de overeenkomst

4.1 Overeengekomen termijnen voor levering en/of andere prestaties gelden als vast en fataal, tenzij schriftelijk anders overeengekomen. Indien niet binnen de overeengekomen termijnen is gepresteerd, is Leverancier zonder nadere ingebrekestelling in verzuim, tenzij Leverancier bewijst dat het niet halen van de termijnen niet aan Leverancier is toe te rekenen.

4.2 De in artikel 3.5 bedoelde risicoanalyse kan ook – behoudens bij een aanbesteding als bedoeld in artikel 3.6 – eerst na totstandkoming van de Overeenkomst, doch voorafgaand aan de Implementatie, worden uitgevoerd. Indien het voorstel van Leverancier over de wijze waarop met gesignaleerde risico's wordt omgegaan voor Opdrachtgever niet aanvaardbaar is, is Opdrachtgever gerechtigd de Overeenkomst per direct te ontbinden, zonder schadeplichtig te zijn, doch tegen vergoeding van de tot dan toe door Leverancier gemaakte kosten (waaronder de kosten voor het uitvoeren van de risicoanalyse).

4.3 Voor zover uit de Overeenkomst voortvloeit dat Leverancier het transport van de bij de ICT Prestatie behorende zaken verzorgt, rust het risico van beschadiging of verlies gedurende het transport bij Leverancier.

4.4 Opdrachtgever zal zijn verplichtingen uit de Overeenkomst en de daar-

mee samenhangende nadere overeenkomsten (Implementatieplan, SLA, etc.) nakomen en steeds de vereiste medewerking verlenen.

Artikel 5. Implementatie ICT Prestatie

5.1 Tenzij in de Overeenkomst uitdrukkelijk anders is bepaald, of de ICT Prestatie naar zijn aard niet geïmplementeerd kan worden, zal Leverancier zorgdragen voor de Implementatie van de ICT Prestatie in de organisatie van Opdrachtgever, overeenkomstig het (voor zover van toepassing) hieromtrent bepaalde in de Overeenkomst en het Implementatieplan.

5.2 Indien er ten tijde van ondertekening van de Overeenkomst nog geen Implementatieplan is opgesteld, zal dit op eerste verzoek van een der partijen binnen redelijke termijn alsnog in onderling overleg tussen partijen worden opgesteld. Leverancier is penvoerder van het Implementatieplan. De kosten voor het opstellen van het Implementatieplan liggen besloten in de Vergoeding.

5.3 Indien wordt overgegaan tot het opstellen van een Implementatieplan, zal dit plan het navolgende vermelden (voor zover van toepassing):

i) Gedetailleerde beschrijving van de doelstellingen van het project om te komen tot de Implementatie van de ICT Prestatie alsmede de randvoorwaarden en de geldende kaders en normen, mede in het licht van de uitgevoerde risicoanalyse;

ii) De projectorganisatie inclusief de wijze van verslaglegging en de wijze van projectmanagement;

iii) De werkverdeling en verdeling van verantwoordelijkheden, waaronder de van Opdrachtgever verlangde inzet en beschikbaarheid;

iv) Een overzicht van de benodigde Koppelingen, de functionele specificaties daarvan en de eventuele medewerking van derde partijen die voor het aanleggen daarvan vereist is;

v) De deelleveringen (‘milestones’) van het project en de functionele specificaties voor de deelleveringen waaraan moet worden voldaan (in relatie tot het Overeengekomen gebruik);

vi) Het tijdschema van de Implementatie (inclusief de deelleveringen), overeenkomstig de eisen die in de Overeenkomst aan de planning zijn gesteld;

vii) De wijze waarop iedere deellevering wordt opgeleverd;

viii) De wijze waarop de Acceptatieprocedure zal worden uitgevoerd;

ix) De wijze waarop de Conversie zal plaatsvinden;
x) De wijze waarop Opdrachtgever middels opleidingen/trainingen vertrouwd zal worden gemaakt met het gebruik en het (technisch en functioneel) beheer van de ICT Prestatie, voor zover overeengekomen.

5.4 Indien tijdens de Implementatie blijkt dat aanpassingen aan het Applicatielandschap noodzakelijk zijn die Leverancier niet heeft voorzien in het aanbod en/of de in artikel 3.5 bedoelde risicoanalyse, doch wel had behoren te voorzien, komen de kosten voor de betreffende aanpassingen voor rekening van Leverancier.

5.5 Tenzij anders overeengekomen zijn tussentijdse opleverdata, in afwijking van artikel 4.1, niet fataal, doch is de in de Overeenkomst en/of het Implementatieplan opgenomen einddatum voor de Implementatie wel fataal.

5.6 Leverancier verklaart zich reeds nu voor alsdan bereid en in staat om na afloop van de (initiële) Implementatie, op verzoek van Opdrachtgever, gedurende de looptijd van de Overeenkomst aan de Implementatie gerelateerde werkzaamheden te verrichten. Deze werkzaamheden zullen alsdan worden verricht tegen de in de Overeenkomst daartoe vermelde tarieven (met inachtneming van artikel 9.6) dan wel, bij gebreke daarvan, tegen de gebruikelijke tarieven van Leverancier. Artikel 5 is van overeenkomstige toepassing op deze werkzaamheden.

Artikel 6. Gemeentelijke ICT-kwaliteitsnormen, Interoperabiliteitseisen en standaarden

6.1 Tot het Overeengekomen gebruik behoort dat de ICT Prestatie voldoet aan de:

i) ten tijde van het sluiten van de Overeenkomst voor de functie en het werkingsgebied van de betreffende ICT Prestatie gepubliceerde Gemeentelijke ICT-kwaliteitsnormen;
ii) in de Overeenkomst (nader) gespecificeerde overige Gemeentelijke ICT-kwaliteitsnormen en/of Interoperabiliteitseisen, dan wel andere normen en standaarden.

6.2 Leverancier voert voorafgaand aan de Implementatie de preventieve testen uit die in voornoemde normen zijn voorgeschreven. Deze testen worden uitgevoerd op een omgeving van Leverancier. Leverancier overlegt het testrapport waaruit blijkt dat de ICT Prestatie aan voornoemde norm(en) voldoet.

6.3 Leverancier is niet verplicht de in het vorige lid bedoelde preventieve testen uit te voeren indien hij een rapportage kan overleggen waaruit blijkt dat voornoemde testen reeds in positieve zin zijn afgerond op exact dezelfde versie van de ICT Prestatie en met vergelijkbaar Overeengekomen gebruik.

6.4 Gedurende de Acceptatieprocedure zal worden getoetst in hoeverre de ICT Prestatie na Implementatie bij Opdrachtgever daadwerkelijk voldoet aan hetgeen in artikel 6.1 is benoemd.

6.5 Indien en voor zover de ICT Prestatie mede bestaat uit Koppelingen, zal – als onderdeel van de Acceptatieprocedure – een ketentest worden uitgevoerd. Daarbij worden alle Koppelingen tussen de ICT Prestatie en het Applicatielandschap getest op de overeengekomen interoperabiliteit.

6.6 Opdrachtgever is verantwoordelijk voor het tijdig betrekken van de leveranciers van onderdelen van het Applicatielandschap die bij de in het vorige lid bedoelde ketentest worden betrokken. De verantwoordelijkheid voor het coördineren van de werkzaamheden van alle betrokken partijen ligt, tenzij anders overeengekomen, bij Leverancier.

6.7 Indien de in artikel 6.5 bedoelde ketentest niet slaagt, en Leverancier aantoont dat dit niet aan hem toerekenbaar is, dan zal een overleg plaatsvinden met alle betrokken partijen teneinde nadere afspraken te maken om te komen tot een passende oplossing. Het initiatief voor dit overleg wordt genomen door de partij die op grond van het vorige lid de coördinatiewerkzaamheden verricht. De Acceptatieprocedure wordt gedurende voornoemd overleg opgeschort. Zodra partijen overeenstemming hebben bereikt over de passende oplossing, zullen zij deze vastleggen in een (gewijzigd of aanvullend) Implementatieplan. Artikel 5 is van overeenkomstige toepassing op het opstellen/wijzigen van dit plan. Voor zover het uitvoeren van dit plan leidt tot meerwerk, zal dit niet aanvangen dan na uitdrukkelijke instemming van Opdrachtgever.

Artikel 7. Acceptatie

7.1 Indien er geen Implementatieplan is opgesteld, of dit plan geen beschrijving bevat van de wijze waarop de Acceptatieprocedure wordt uitgevoerd, zal op eerste verzoek van Opdrachtgever alsnog in een schriftelijk testprotocol worden vastgelegd op welke wijze de Acceptatieprocedure zal worden uitgevoerd. Artikel 5.2 is van overeenkomstige toepassing op het opstellen van dit testprotocol.

7.2 Tenzij in de Overeenkomst, het Implementatieplan of het in het vorige lid bedoelde testprotocol anders is bepaald, is de Acceptatieprocedure als volgt:

i) Na iedere levering van (delen van) de ICT Prestatie, wordt de betreffende levering getest op Gebreken. Door partijen wordt daarbij een testverslag opgemaakt en ondertekend. In dit testverslag zal worden vastgelegd of de ICT Prestatie Gebreken vertoont en voorts of de ICT Prestatie (deels) is goedgekeurd, dan wel afgekeurd;

ii) Binnen een redelijke termijn, althans de daartoe in de Overeenkomst gespecificeerde termijn, na de datum van de ondertekening van het testverslag, zal Leverancier een planning afgeven waarbinnen de in het testverslag vastgelegde Gebreken voor eigen rekening worden verholpen;

iii) Leverancier zal na afloop van de in het vorige lid bedoelde termijn (het gedeelte van) de bijgewerkte ICT Prestatie opnieuw ter Acceptatie middels de Acceptatieprocedure voorleggen.

7.3 De in het kader van de Acceptatieprocedure gehanteerde termijnen en (bijgestelde) planningen dienen te passen in de algehele planning van de Overeenkomst of het Implementatieplan en mogen niet tot vertraging leiden.

7.4 Indien (delen van) de ICT Prestatie bij het voor de tweede maal doorlopen van de (integrale) Acceptatieprocedure op Gebreken wordt/worden afgekeurd, is Opdrachtgever gerechtigd om:

i) de Overeenkomst – geheel of gedeeltelijk – zonder nadere ingebrekestelling buiten rechte te ontbinden, waarbij geldt dat Leverancier dan tevens binnen de kaders van artikel 13 aansprakelijk is voor de door Opdrachtgever geleden en te lijden schade; of

ii) onverminderd zijn recht op vergoeding (binnen de kaders van artikel 13) van de reeds geleden schade Leverancier toe te staan

de Gebreken alsnog voor diens rekening te herstellen; of

iii) de ICT Prestatie onder een nader overeen te komen voorwaarde voorwaardelijk te accepteren, waarbij geldt dat indien Leverancier niet tijdig aan de bij de voorwaardelijke acceptatie gestelde voorwaarden voldoet, het bepaalde onder i van toepassing is.

7.5 Voor Gebreken die niet binnen de overeengekomen planning kunnen worden opgelost, kan met wederzijds goedvinden worden besloten om tijdelijk een acceptabele work-around aan te brengen en/of om hiervoor later een oplossing te vinden.

7.6 Gebreken die (individueel noch gezamenlijk) niet in de weg staan aan het gebruik voor productieve doeleinden van (het betreffende onderdeel van) de ICT Prestatie, kunnen geen grond vormen voor niet-Acceptatie, onverminderd de verplichting van Leverancier om die op korte termijn te herstellen.

7.7 Indien de ICT Prestatie in deelleveringen wordt geleverd, vindt na iedere levering een Acceptatieprocedure plaats en vindt na Acceptatie van het laatste deel van de ICT Prestatie vervolgens een integrale Acceptatieprocedure plaats, waarbij de gehele ICT Prestatie alsmede de samenhang van deelleveringen (‘som der delen’) op Gebreken wordt getoetst. Er is pas sprake van Acceptatie na het succesvol doorlopen van de integrale Acceptatieprocedure.

7.8 Acceptatie wordt geacht te hebben plaatsgevonden indien er geen Acceptatieprocedure is afgesproken noch heeft plaatsgevonden en Opdrachtgever de ICT Prestatie voor productieve doeleinden in gebruik heeft genomen binnen zijn organisatie.

Artikel 8. Onderhoud en ondersteuning

Algemeen

8.1 Tenzij anders overeengekomen, verricht Leverancier Onderhoud aan de ICT Prestatie tegen de in de Overeenkomst beschreven vergoeding. Het Onderhoud gaat in vanaf de Acceptatie van (het betreffende deel van) de ICT Prestatie.

8.2 De hierna te beschrijven voorwaarden gelden als (minimum) voorwaarden voor Onderhoud, tenzij hiervan in de Overeenkomst / SLA is afgeweken.

8.3 Het Onderhoud omvat, tenzij anders overeengekomen, ten minste de volgende diensten:
   i) Correctief Onderhoud;
   ii) Preventief Onderhoud;
   iii) Innovatief Onderhoud;
   iv) Gebruikersondersteuning.

8.4 Het moment van het verrichten van Onderhoud wordt in onderling overleg bepaald. Uitgangspunt daarbij is dat Onderhoud op zodanige wijze plaatsvindt dat dit minst verstorend is voor de bedrijfsprocessen van Opdrachtgever. Onderhoud dat verstorend is of kan werken voor de bedrijfsprocessen van Opdrachtgever wordt bovendien tijdig vooraf aangekondigd.

Bereikbaarheid

8.5 Leverancier is in het kader van Onderhoud ieder geval bereikbaar op werkdagen tussen 08.00-18.00 uur.

Service level agreement

8.6 Leverancier verklaart zich bereid om – indien en voor zover zulks niet reeds geregeld is in de Overeenkomst – op eerste verzoek van Opdrachtgever een of meer service level agreements (SLA's) te sluiten, waarin concrete Service Levels ter zake van het in artikel 8.3 bedoelde Onderhoud worden vastgelegd en waarin maatregelen zijn opgenomen ter zake van het al dan niet halen van de afgesproken Service Levels.

8.7 De gevolgen van het niet halen van Service Levels worden in de Overeenkomst/SLA geregeld, met dien verstande dat (gedeeltelijke) ontbinding van de Overeenkomst en/of de SLA('s) in ieder geval mogelijk is bij het meerdere meetperiodes achtereenvolgens niet halen van dezelfde Service Levels. Eventueel in de SLA bedongen maatregelen laten de overige rechten van Opdrachtgever onverlet, waaronder begrepen het recht om naast de maatregel de door hem geleden schade te verhalen. Betaalde sancties (als onderdeel van de afgesproken maatregelen) worden in mindering gebracht op de eventueel te betalen schadevergoeding.

8.8 Indien en voor zover Leverancier bewijst dat een Gebrek niet aan hem toerekenbaar is, is hij niet verplicht tot herstel daarvan. Indien

Opdrachtgever niettemin opdracht geeft tot voornoemd herstel, is Leverancier gerechtigd de kosten gemoeid met het herstel separaat door te berekenen.

Preventief en Innovatief Onderhoud

8.9 In het kader van Preventief en/of Innovatief Onderhoud garandeert Leverancier ten minste:

i) dat de ICT Prestatie steeds tijdig zal blijven voldoen aan de relevante Wet- en regelgeving;

ii) dat de ICT Prestatie steeds tijdig geschikt zal blijven voor gegevensuitwisseling met de overige relevante onderdelen van het Applicatielandschap (voor zover bekend bij Leverancier) en in dat kader aan de overeengekomen Interoperabiliteitseisen zal blijven voldoen;

iii) dat de ICT Prestatie door middel van het tijdig uitbrengen van Updates en/of Upgrades steeds tijdig zal blijven voldoen aan nieuwe versies van de Gemeentelijke ICT-kwaliteitsnormen die in de Overeenkomst als vereiste normen zijn gespecificeerd;

iv) dat bij het uitbrengen van Updates en/of Upgrades de performance van de ICT Prestatie ten minste gelijk blijft en dat de ICT Prestatie blijft voldoen aan het Overeengekomen gebruik.

8.10 Op verzoek van Opdrachtgever verzorgt Leverancier de Implementatie van Updates en Upgrades, tegen een nader overeen te komen vergoeding. De bepalingen omtrent Implementatie en Acceptatie zijn in dat geval van overeenkomstige toepassing, met dien verstande dat bij Implementatie van een Update in beginsel geen Acceptatieprocedure zal plaatsvinden.

8.11 Opdrachtgever is – behoudens in de situatie als bedoeld in artikel 31.4 – gerechtigd het gebruik en/of de Implementatie van Updates en Upgrades te weigeren, zonder dat dit afbreuk doet aan het door Leverancier te verlenen Onderhoud, met dien verstande dat:

i) er geen sprake is van een tekortkoming van Leverancier in het kader van Onderhoud indien een bepaald Gebrek in een Update en/of Upgrade is verholpen en Opdrachtgever de ingebruikname van die Update of Upgrade weigert;

ii) Opdrachtgever maximaal 24 maanden mag achterlopen in het

ingebruiknemen van Update en/of Upgrade, bij gebreke waarvan Leverancier na het verstrijken van die periode gerechtigd is de aantoonbare meerkosten voor het blijvend moeten verlenen van Onderhoud op (het betreffende onderdeel van) de door Opdrachtgever gebruikte ICT Prestatie in rekening te brengen.

Rapportage en controle

8.12 Leverancier zal periodiek aan Opdrachtgever rapport uitbrengen over de nakoming door hem van de overeengekomen Service Levels, waaronder in ieder geval wordt verstaan de beschikbaarheid van de ICT Prestatie en het niveau van de diensten, waaronder het Onderhoud van de ICT Prestatie alsmede het geplande Innovatief Onderhoud. De inhoud en frequentie van deze rapportage is nader omschreven in de SLA.

8.13 Na ontvangst van het rapport zal door Opdrachtgever worden vastgesteld of Leverancier zijn verplichtingen uit hoofde van het Onderhoud, waaronder de door hem gegarandeerde Service Levels, heeft gehaald, al dan niet door inschakeling van een derde overeenkomstig artikel 21.

Latere onderhoudsovereenkomst

8.14 Leverancier verklaart zich reeds nu voor alsdan bereid om, voor zover oorspronkelijk is overeengekomen dat Leverancier geen of slechts onderdelen van het in artikel 8.3 bedoelde Onderhoud verricht, op eerste verzoek van Opdrachtgever alsnog in overleg te treden om te komen tot een Overeenkomst voor het verrichten van aanvullende diensten ten aanzien van Onderhoud.

Artikel 9. Vergoeding, facturatie en betaling

9.1 De door Opdrachtgever ten behoeve van de ICT Prestatie aan Leverancier te betalen vergoedingen zijn vastgelegd in de Overeenkomst.

9.2 De facturering van de vergoedingen vindt, tenzij anders overeengekomen, als volgt plaats:

i) Implementatie- of ontwikkelingskosten: van de totale vergoeding is 30% eerst opeisbaar na integrale Acceptatie, over de resterende 70% kunnen in de Overeenkomst nadere afspraken worden gemaakt;

ii) De kosten van de Gebruiksrechten voor Programmatuur:

(1) voor zover het betreft Derdenprogrammatuur: 100% bij levering;
(2) voor zover het geen Derdenprogrammatuur betreft: 70% bij ingebruikname voor productieve doeleinden en 30% na integrale Acceptatie;

iii) De kosten van Onderhoud van de ICT Prestatie:
(1) voor zover het eenmalige vergoedingen betreft: eerst na integrale Acceptatie;
(2) en voor zover het periodieke vergoedingen betreft: periodiek vooraf, voor het eerst na integrale Acceptatie;

iv) Overige zaken en diensten: Facturatie na Acceptatie van de desbetreffende ICT Prestatie, of maandelijks achteraf op basis van werkelijk bestede uren in het geval de dienstverlening op nacalculatiebasis wordt uitgevoerd.

9.3 Een factuur dient te voldoen aan de wettelijke eisen alsmede de eisen die in de Overeenkomst worden gesteld.

9.4 De betalingstermijn bedraagt 30 dagen na ontvangst factuur, tenzij anders overeengekomen.

9.5 Leverancier verzendt de factuur elektronisch overeenkomstig de geldende eisen voor facturatie zoals opgenomen in de Gemeentelijke ICT-kwaliteitsnormen, tenzij anders tussen partijen overeengekomen.

9.6 Jaarlijks per 1 januari kunnen de overeengekomen (jaar)tarieven en doorlopende vergoedingen door Leverancier worden aangepast, mits deze minimaal één maand voorafgaand is aangekondigd. Deze wijziging is gelimiteerd tot maximaal de (eventuele) wijziging van het laatst gepubliceerde prijsindexcijfer voor 'Computerprogrammering, advisering en aanverwante diensten' (CPA: 62) zoals opgenomen in de door het Centraal Bureau voor de Statistiek (CBS) gepubliceerde tabel 'Dienstenprijzen; commerciële dienstverlening index (2010=100)', althans de opvolger daarvan.

9.7 Leverancier is voorts gerechtigd de aantoonbare prijsstijging van Derdenprogrammatuur per 1 januari door te belasten, mits deze prijsstijging ten tijde van het sluiten van de Overeenkomst nog niet voorzienbaar was. Indien de prijzen van Derdenprogrammatuur gedurende de looptijd van de Overeenkomst dalen, zal Leverancier van Derdenprogrammatuur steeds slechts de actuele (verlaagde) prijs in rekening brengen.

9.8 Indien en voor zover de vergoeding en/of het aantal Gebruiksrechten voor het gebruik van de ICT Prestatie afhankelijk is gesteld van een aan Opdrachtgever gerelateerd getal dat aan wijziging onderhevig is (zoals inwoneraantal, oppervlakte werkgebied, etc.), dan zal deze vergoeding / het aantal verleende Gebruiksrechten slechts éénmaal per jaar en wel per 1 januari worden bijgesteld.

9.9 Het bepaalde in dit artikel omtrent Derdenprogrammatuur geldt alleen voor zover Leverancier heeft voldaan aan het bepaalde in artikel 19.1.

Artikel 10. Garanties

10.1 Leverancier garandeert dat:

i) de ICT Prestatie de overeengekomen eigenschappen zal bevatten en voldoet aan het Overeengekomen gebruik;

ii) hij alleen Personeel inzet dat beschikt over de overeengekomen dan wel voor het verrichten van de ICT Prestatie benodigde vaardigheden en kwalificaties, rekening houdend met de aard van de te leveren ICT Prestatie en de wijze waarop Leverancier zich als deskundige heeft gepresenteerd. Hij garandeert tevens dat het door hem ingezette personeel voldoet aan de eisen die dienaangaande aan een vergelijkbare dienstverlener als redelijk bekwaam en redelijk handelend vakgenoot mogen worden gesteld;

iii) hij ten minste tot 2 jaar na datum van Acceptatie Onderhoud kan plegen op de ICT Prestatie;

iv) de ICT Prestatie geschikt zal zijn voor gebruik in samenhang met het Applicatielandschap (voor zover bij Leverancier bekend of bekend had moeten zijn);

v) de ICT Prestatie voldoet en (bij Onderhoud) zal blijven voldoen aan de relevante wet- en regelgeving en de Gemeentelijke ICT-kwaliteitsnormen.

10.2 Indien Opdrachtgever tijdens de looptijd van de Overeenkomst op enig tijdstip constateert dat de ICT Prestatie of delen daarvan niet voldoen aan voornoemde garanties, zal Opdrachtgever Leverancier hiervan schriftelijk of per email en in spoedgevallen ook telefonisch op de hoogte stellen. Indien Leverancier van mening is dat Opdrachtgever geen beroep kan doen op de garantiebepalingen, omdat een Gebrek niet behoort tot de gegarandeerde eigenschappen of terug te voeren is

op niet aan Leverancier toe te rekenen oorzaken of op niet door Leverancier geleverde of geadviseerde Programmatuur of apparatuur, rust de bewijslast terzake op Leverancier.

Artikel 11. Documentatie

11.1 Leverancier zal Opdrachtgever voorzien van voldoende en begrijpelijke documentatie over de eigenschappen, technische inpasbaarheid en gebruiksmogelijkheden van de ICT Prestatie. De documentatie voor eindgebruikers is in de Nederlandse taal opgesteld, overige documentatie mag ook in het Engels zijn gesteld (tenzij anders overeengekomen). De documentatie zal zodanig zijn en blijven:

i) dat zij een juiste, volledige en gedetailleerde beschrijving geeft van de door Leverancier te leveren ICT Prestatie, alsmede de functies daarvan;

ii) dat zij een juiste en volledige beschrijving geeft van de door de Leverancier in het kader van de Implementatie of het Onderhoud gemaakte instellingen/parametriseringen;

iii) dat gebruikers van alle mogelijkheden van de ICT Prestatie gebruik kunnen maken en de werking ervan goed kunnen begrijpen;

iv) dat zij geschikt is om op basis hiervan de ICT Prestatie te kunnen testen in het kader van een Acceptatieprocedure;

v) dat zij geschikt is om op basis hiervan de ICT Prestatie adequaat te kunnen beheren en te kunnen inpassen in het Applicatielandschap overeenkomstig de documentatie-eisen over inpasbaarheid uit de Gemeentelijke ICT-kwaliteitsnormen.

11.2 De relevante documentatie zal steeds tijdig voor de desbetreffende Acceptatieprocedure aan Opdrachtgever ter beschikking worden gesteld, tenzij anders overeengekomen. Bij het leveren van Updates of Upgrades of het leveren van aanvullende programmatuur, zal steeds bij de terbeschikkingstelling daarvan de documentatie met betrekking daarop worden meegeleverd.

11.3 Leverancier zal de documentatie steeds actueel houden. Zodra blijkt dat de documentatie niet of niet langer juist of volledig is, zal Leverancier de documentatie zo spoedig mogelijk en op zijn kosten actualiseren.

Artikel 12. Productmanagement

12.1 Onverminderd het eventueel overeengekomen Onderhoud zal Leverancier Opdrachtgever periodiek en tijdig informeren over de planning en beoogde functionaliteiten voor Upgrades (soms 'roadmap' genoemd).

12.2 Voor zover Leverancier een (fysiek of virtueel) orgaan of platform faciliteert ten behoeve van (een deel van) zijn klanten voor het delen van kennis en ervaring over de ICT Prestatie en/of het bespreken van de (te verwachten) ontwikkelingen van de ICT Prestatie, zal Leverancier Opdrachtgever daar kosteloos en zonder beperkingen toegang toe verlenen.

12.3 Indien Leverancier – hetzij ten behoeve van Opdrachtgever, hetzij ten behoeve van derden – een aanvulling op bestaande Programmatuur heeft ontwikkeld waarop artikel 17.4 GIBIT, althans een daarmee vergelijkbare bepaling, van toepassing is, dan:

i) zal Leverancier Opdrachtgever en andere gebruikers van de Programmatuur over deze aanvulling informeren, waaronder of deze aanvulling zal worden opgenomen in de (op een later moment) te verschijnen Updates of Upgrades en welke consequenties verbonden zijn aan de ingebruikname van de aanvulling; en

ii) zal Leverancier – onverminderd eventueel overeengekomen Onderhoud – deze aanvulling om niet ter beschikking stellen aan Opdrachtgever en andere gebruikers van de Programmatuur; en

iii) is het gebruik van de betreffende aanvulling voor risico van Opdrachtgever, tenzij:

(1) de aanvulling in opdracht van Opdrachtgever is ontwikkeld; of

(2) de aanvulling in het kader van Onderhoud als onderdeel van een Update of Upgrade aan Opdrachtgever ter beschikking wordt gesteld.

Artikel 13. Aansprakelijkheid

13.1 De partij die toerekenbaar tekortschiet in de nakoming van zijn verplichtingen, is tegenover de andere partij aansprakelijk voor de door deze geleden en/of te lijden schade, met inachtneming van het bepaalde in artikel 20.9 en het bepaalde in het onderhavige artikel.

13.2 De aansprakelijkheid voor schade, uit welke hoofde dan ook, is – tenzij anders overeengekomen – beperkt tot vier maal de hoogte van de

Vergoeding per gebeurtenis, met dien verstande dat de aansprakelijkheid nooit meer zal bedragen dan € 5.000.000,– per gebeurtenis. Samenhangende gebeurtenissen worden daarbij aangemerkt als één gebeurtenis. Louter de volgende schadeposten komen voor vergoeding in aanmerking:

i) schade aan de ICT Prestatie en/of aan gegevensbestanden, waaronder in elk geval verstaan wordt: materiële beschadiging, gebrekkig of niet functioneren, verminderde betrouwbaarheid en verhoogde storingsgevoeligheid;
ii) schade aan andere eigendommen van partijen en/of van derden;
iii) kosten van noodzakelijke wijzigingen en/of veranderingen in de ICT Prestatie, aangebracht ter beperking of herstel van schade;
iv) de kosten van noodvoorzieningen, zoals het uitwijken naar andere computersystemen, het inhuren van derden of het hanteren van noodprocedures of afwijkende werkwijzen;
v) kosten, waaronder begrepen personeelskosten, van het noodgedwongen langer operationeel houden van oude systemen en daarmee samenhangende voorzieningen;
vi) de kosten van het niet kunnen inzetten (leegloop) van medewerkers, goederen en faciliteiten van Opdrachtgever en de kosten van het niet kunnen inzetten (leegloop) van door Opdrachtgever in het kader van de uitvoering van de Overeenkomst ingehuurde derden, voorzover deze kosten, in redelijkheid, niet vermijdbaar zijn;
vii) de kosten voor het herstel van Gebreken van Opdrachtgever of door hem ingeschakelde derden, of alle extra kosten verbonden aan de noodgedwongen vroegtijdige vervanging van de ICT Prestatie door een systeem van een derde Leverancier;
viii) aan derden aantoonbaar verschuldigde vergoedingen en boetes alsmede de waarde van het verloren gaan van door derden verstrekte garanties;
ix) redelijke kosten gemaakt ter voorkoming of beperking van schade, die als gevolg van de gebeurtenis waarop de aansprakelijkheid berust, mocht worden verwacht;
x) redelijke kosten gemaakt ter vaststelling van de schadeoorzaak, de aansprakelijkheid, de hoogte van de schade en de wijze van herstel.

13.3 De in het vorige lid bedoelde beperking van aansprakelijkheid komt te vervallen:
   i) in geval van aanspraken van derden op schadevergoeding ten gevolge van dood of letsel en/of;
   ii) indien sprake is van opzet of grove schuld aan de zijde van de andere partij of diens Personeel; en/of
   iii) in geval van schending van intellectuele eigendomsrechten als bedoeld in artikel 17.

13.4 Indien er als gevolg van een toerekenbare tekortkoming van Leverancier, of een aan Leverancier toerekenbaar gedragen of nalaten, aan Opdrachtgever door een overheidstoezichthouder een boete wordt opgelegd, welke boete (deels) rechtstreeks verband houdt met voornoemde tekortkoming, gedragen of nalaten, vrijwaart Leverancier Opdrachtgever voor (dat deel van) die boete. De vrijwaring geldt niet voor zover de boete (mede) verband houdt met gedrag van Opdrachtgever zelf (zoals het gebruik van de ICT Prestatie). Op deze vrijwaring zijn de voorgaande beperkingen van aansprakelijkheid niet van toepassing.

13.5 Alle verplichtingen, ook die krachtens de belasting-, zorgverzekerings- en sociale verzekeringswetgeving met betrekking tot Personeel van Leverancier, komen ten laste van Leverancier. Leverancier vrijwaart Opdrachtgever tegen elke aansprakelijkheid die daarmee verband houdt. Op deze vrijwaring zijn de voorgaande beperkingen van aansprakelijkheid niet van toepassing.

Artikel 14. Verzekering

14.1 Leverancier heeft zich op een naar verkeersnormen passende en gebruikelijke wijze verzekerd en houdt zich zodanig verzekerd tegen alle aansprakelijkheid voortvloeiende uit de Overeenkomst en de onderhavige voorwaarden, waaronder in ieder geval begrepen beroeps- en bedrijfsaansprakelijkheid, althans biedt anderszins aantoonbaar voldoende waarborgen ter dekking van eventuele aansprakelijkheid.

14.2 De in het vorige lid bedoelde verzekering/waarborg biedt dekking voor ten minste 200% van het in artikel 13.2 bedoelde bedrag per jaar.

Artikel 15. Geheimhouding

15.1 Partijen maken hetgeen hen bij de uitvoering van de Overeenkomst ter kennis komt, en waarvan zij het vertrouwelijke karakter kennen of redelijkerwijs kunnen vermoeden, tot minimaal twee jaar na afloop van de Overeenkomst, op geen enkele wijze verder bekend behalve voorzover enig wettelijk voorschrift, onderzoek door een bevoegde toezichthouder of uitspraak van de rechter of een door partijen aangewezen geschillenbeslechter hen tot bekendmaking daarvan verplicht. De inhoud van de onder de GIBIT gesloten Overeenkomst(en) als zodanig mag/mogen met andere gemeenten, aan gemeenten gelieerde rechtspersonen en gemeentelijke samenwerkingsverbanden worden gedeeld.

15.2 Partijen verplichten hun personeel en andere ingeschakelde hulppersonen om de geheimhoudingsverplichting opgenomen in het vorige lid na te komen.

15.3 Partijen geven alle gegevens die zij van elkaar hebben ontvangen en die vertrouwelijk van aard zijn op eerste verzoek terug.

15.4 De partij die in dit artikel opgenomen geheimhoudingsverplichting schendt, is aan de andere partij een onmiddellijk opeisbare boete verschuldigd van 4 keer de Vergoeding per overtreding, onverminderd het recht de daadwerkelijk geleden schade te verhalen (met inachtneming van artikel 13). De hiervoor bedoelde boete bedraagt evenwel nooit meer dan € 50.000,- per overtreding.

Artikel 16. Overmacht

16.1 Een tekortkoming in de nakoming van de Overeenkomst, die niet te wijten is aan schuld van een partij en evenmin krachtens, wet, rechtshandeling of in het maatschappelijk rechtsverkeer geldende opvatting voor rekening van de betreffende partij komt, levert overmacht op.

16.2 Onder overmacht aan de zijde van Leverancier wordt in ieder geval niet verstaan: gebrek aan Personeel, stakingen, ziekte van Personeel (m.u.v. pandemie), verlate aanlevering of ongeschiktheid van voor het verrichten van de ICT Prestatie benodigde goederen dan wel liquiditeits- of solvabiliteitsproblemen. Een aantoonbare storing van nuts-/telecomvoorzieningen wordt wel als overmacht beschouwd, tenzij deze veroorzaakt is door Leverancier of de ICT Prestatie juist ziet op het beschikbaar houden van voornoemde voorzieningen.

Artikel 17. Intellectuele eigendom

17.1 Tenzij anders overeengekomen, berusten alle rechten van intellectuele eigendom op de krachtens de Overeenkomst door Leverancier ontwikkelde en ter beschikking gestelde ICT Prestaties uitsluitend bij Leverancier of diens licentiegever(s).

17.2 Alle rechten op de met de ICT Prestatie van Opdrachtgever afkomstige verwerkte gegevens (blijven) rusten bij Opdrachtgever, ongeacht waar deze gegevens staan opgeslagen en ongeacht of de gegevens na initiële ontvangst zijn bewerkt of niet.

17.3 Leverancier verleent, behoudens andersluidende afspraken in de Overeenkomst, een Gebruiksrecht op de ICT Prestaties. Indien voor het Gebruiksrecht periodiek een vergoeding verschuldigd is, is de duur van het Gebruiksrecht gelijk aan de looptijd van de Overeenkomst. In overige gevallen is het Gebruiksrecht eeuwigdurend en onherroepelijk. Het Gebruiksrecht omvat in ieder geval het recht de ICT Prestatie(s) (en alle daarin besloten liggende informatie/kennis) te gebruiken voor het Overeengekomen gebruik, alsmede voor testdoeleinden, met inbegrip van alle daarvoor redelijkerwijs noodzakelijke al dan niet tijdelijke verveelvoudigingen en openbaarmakingen.

17.4 Indien de Overeenkomst (mede) ziet op het door Leverancier ontwikkelen van een aanvulling op bestaande Programmatuur, dan geldt voor die aanvulling eveneens het bepaalde in lid 3, met dien verstande dat Leverancier – tenzij anders overeengekomen – de betreffende aanvulling om niet overeenkomstig het bepaalde in artikel 12.3 aan andere gebruikers van de Programmatuur zal aanbieden.

17.5 Indien de Overeenkomst (mede) ziet op het door Leverancier ontwikkelen van Programmatuur, niet zijnde een aanvulling op bestaande Programmatuur, dan berusten de rechten van intellectuele eigendom op die te ontwikkelen Programmatuur – in afwijking van artikel 17.1 en 17.3 – bij Opdrachtgever. Voor zover nodig worden de betreffende rechten reeds nu voor alsdan overgedragen door Leverancier aan Opdrachtgever, die deze overdracht reeds nu voor alsdan aanvaardt. Deze overdracht ziet op alle huidige en toekomstige rechten in de meest ruime zin van het woord. Leverancier doet reeds nu voor alsdan voorts – voor zover de wet dat toestaat – onherroepelijk afstand van eventuele persoonlijkheidsrechten op de ICT Prestaties. Leverancier zal voorts

alle broncodes van de betreffende ontwikkelde Programmatuur aan Opdrachtgever ter beschikking stellen. De eenmalige koopprijs voor deze overdracht wordt geacht besloten te hebben gelegen in de Vergoeding. De overdracht en de levering van de rechten en eerder genoemde broncode vindt plaats onder de opschortende voorwaarde van betaling van de betreffende Vergoeding.

17.6 Opdrachtgever verklaart zich reeds nu voor alsdan bereid in gesprek te gaan over het tegen een vergoeding mogelijk (gedeeltelijk) terug overdragen van de in het vorige lid bedoelde rechten, waarbij Leverancier dan gelijktijdig met deze (terug)overdracht een Gebruiksrecht overeenkomstig lid 3 verleent op de aldus overgedragen rechten.

17.7 Leverancier garandeert dat de door hem aan Opdrachtgever verstrekte ICT Prestaties geen inbreuk maken op enige intellectuele eigendomsrechten of andere rechten, waaronder persoonlijkheidsrechten, van derden. Leverancier vrijwaart Opdrachtgever en stelt Opdrachtgever schadeloos voor alle aanspraken van derden gebaseerd op de stelling dat door Leverancier aan Opdrachtgever ter beschikking gestelde ICT Prestaties, inbreuk maken op bedoelde rechten van die derden. Indien Opdrachtgever door een derde het recht tot gebruik van de ICT Prestaties of delen daarvan wordt ontzegd, zal Leverancier voor zijn rekening en te harer keuze onverwijld hetzij:

i) zorgen dat Opdrachtgever alsnog het recht verkrijgt het gebruik voort te zetten;
ii) het inbreuk makende onderdeel vervangen door een ander onderdeel met gelijkwaardige gebruiksmogelijkheden, dat geen inbreuk maakt op dergelijke rechten van derden;
iii) het inbreuk makende onderdeel zodanig wijzigen dat de inbreuk wordt opgeheven.

17.8 Bij vervanging of wijziging als onder (ii) en (iii) bedoeld, zal de functionaliteit van de vervangende onderdelen minimaal gelijkwaardig zijn aan de vervangen onderdelen en zullen de garanties van artikel 10 volledig in tact blijven.

17.9 In het geval derden Opdrachtgever ter zake van een beweerdelijke schending van intellectuele eigendomsrechten aansprakelijk stellen, is Opdrachtgever – onverminderd het voorgaande – gerechtigd om de Overeenkomst schriftelijk, buiten rechte geheel of gedeeltelijk te ont-

binden. Een dergelijke ontbinding laat de overige rechten van Opdrachtgever onverlet.

Artikel 18. Toegang tot data en autorisaties

18.1 Leverancier stelt Opdrachtgever gedurende de looptijd van de Overeenkomst in staat om te allen tijde toegang te krijgen tot de met de ICT Prestatie ten behoeve van Opdrachtgever verwerkte gegevens, alsmede de daarbij ingestelde (instellingen met betrekking tot) autorisaties.

18.2 Leverancier kan aan de in het vorige beschreven verplichting onder meer voldoen door:

i) aan Opdrachtgever Koppelingen ter beschikking te stellen en de daarbij horende documentatie, teneinde Opdrachtgever in staat te stellen de gegevens / autorisaties middels de Koppelingen op te vragen;

ii) aan Opdrachtgever een juiste, volledige en gedetailleerde beschrijving te geven van de aan de ICT Prestatie ten grondslag liggende datamodellen, teneinde Opdrachtgever in staat te stellen de gegevens zelf te ontsluiten.

18.3 Indien en voor zover door het verlenen van toegang tot de opgeslagen gegevens een bepaalde beveiliging (waaronder begrepen autorisaties) wordt omzeild, zal Leverancier Opdrachtgever daarover informeren en uitdrukkelijk waarschuwen.

18.4 Opdrachtgever is zelf aansprakelijk voor het gebruik van de op grond van artikel 18 verkregen gegevens. Opdrachtgever vrijwaart Leverancier voor eventuele aanspraken van derden die uit dit gebruik voortvloeien.

Artikel 19. Derdenprogrammatuur

19.1 Indien de door Leverancier te leveren Programmatuur en Koppelingen (mede) bestaat uit Derdenprogrammatuur, zal Leverancier dit in het aanbod uitdrukkelijk specificeren. Leverancier zal in dat geval de eventueel toepasselijke licentievoorwaarden ter beschikking stellen.

19.2 Leverancier zal in het in lid 1 bedoelde geval voorts specificeren in hoeverre het mogelijk is de betreffende Derdenprogrammatuur elders te betrekken en in hoeverre de keuze daartoe over te gaan consequenties heeft voor het aanbod van Leverancier.

19.3 Indien en voor zover de ICT Prestatie afhankelijk is van Derdenprogrammatuur, zal Leverancier zulks uitdrukkelijk in het aanbod specificeren. Leverancier zal duidelijk kenbaar maken waar die afhankelijkheid in is gelegen en welke effecten die afhankelijkheid heeft voor (de kwaliteit van) de door Leverancier te verlenen ICT Prestatie.

19.4 Leverancier zal in het kader van Onderhoud tijdig Updates en Upgrades uitbrengen teneinde de compatibiliteit met Derdenprogrammatuur waarvan de ICT Prestatie afhankelijk is te blijven borgen.

19.5 Indien en voor zover Leverancier bewijst dat een Gebrek in de ICT Prestatie wordt veroorzaakt door een fout in Derdenprogrammatuur, wordt het betreffende Gebrek niet als Gebrek beschouwd, tenzij Leverancier de betreffende fout in de Derdenprogrammatuur had behoren te kennen en het effect van de betreffende fout in de eigen ICT Prestatie redelijkerwijs vermeden had kunnen worden. Dit artikel geldt zowel voor de Implementatie, de Acceptatie als het Onderhoud.

19.6 Het in het vorige lid bepaalde laat onverlet dat Leverancier in voorkomend geval binnen de kaders van het Onderhoud alle redelijke inspanningen zal betrachten om zo spoedig mogelijk het Gebrek alsnog op te lossen, bijvoorbeeld door de fout in de Derdenprogrammatuur in de eigen ICT Prestatie te omzeilen en/of door Opdrachtgever zo spoedig mogelijk te voorzien van Updates en/of Upgrades op de ICT Prestatie en/of de Derdenprogrammatuur.

19.7 Het bepaalde in artikel 19.5 is uitsluitend van toepassing indien Leverancier heeft voldaan aan de in artikel 19.1 tot en met 19.3 bedoelde informatieverplichtingen.

19.8 De in het kader van artikel 19.1 meegeleverde licentievoorwaarden prevaleren op hetgeen in de Overeenkomst is bepaald, doch louter voor zover het betreft de Derdenprogrammatuur.

Artikel 20. Opschorting, opzegging en ontbinding

Opschorting

20.1 Leverancier is niet gerechtigd zijn verplichtingen op te schorten dan na het sturen van een ingebrekestelling, waarin aan Opdrachtgever een redelijke termijn van minimaal 30 dagen wordt geboden om alsnog aan de verplichtingen te voldoen.

Opzegging

20.2 Overeenkomsten voor bepaalde tijd kunnen – behoudens de specifieke opzeggingsgronden in de GIBIT of de Overeenkomst – niet tussentijds worden opgezegd (artikel 7:408 lid 1 BW is niet van toepassing). Overeenkomsten voor onbepaalde tijd kunnen worden opgezegd met inachtneming van een opzegtermijn van respectievelijk drie (3) maanden voor Opdrachtgever en achttien (18) maanden voor Leverancier.

20.3 Ook als meerdere Overeenkomsten onderlinge samenhang vertonen (bijv. een licentie- en een onderhoudsovereenkomst), is Opdrachtgever niettemin gerechtigd slechts een deel van de Overeenkomsten (selectief) op te zeggen tegen het einde van de dan actuele looptijd en met inachtneming van een opzegtermijn van drie (3) maanden. Een dergelijke opzegging heeft overigens geen effect op de overige samenhangende Overeenkomsten.

20.4 Opdrachtgever is voorts bevoegd de Overeenkomst en alle daarmee samenhangende overeenkomsten, met inachtneming van een opzegtermijn van twaalf (12) maanden, op te zeggen tegen de datum:

i) dat de rechten en verplichtingen van Opdrachtgever onder algemene titel overgaan op een andere partij (bijv. vanwege een gemeentelijke fusie); of

ii) dat de betreffende activiteiten van Opdrachtgever worden uitbesteed aan een gemeenschappelijke regeling of soortgelijke andere entiteit met een publieke functie.

20.5 Indien Opdrachtgever op grond van ten tijde van het sluiten van de Overeenkomst nog niet voorzienbaar gewijzigd landelijk beleid gehouden is om tegen een bepaalde datum over te stappen op een landelijke voorziening die een (gedeeltelijk) functioneel alternatief vormt voor het met de ICT Prestatie Overeengekomen gebruik, is Opdrachtgever gerechtigd, met inachtneming van een opzegtermijn van twaalf (12) maanden, de Overeenkomst en alle daarmee samenhangende overeenkomsten (voor dat deel) op te zeggen tegen voornoemde datum.

20.6 In geval van opzegging op grond van de artikelen 20.4 en/of 20.5 vindt tussen Opdrachtgever en Leverancier afrekening plaats op basis van de door Leverancier:

i) ter uitvoering van de Overeenkomst ten tijde van de opzegging reeds verrichte werkzaamheden; en

ii) in redelijkheid gemaakte kosten; en
iii) in redelijkheid voor de toekomst reeds aangegane verplichtingen; en
iv) gederfde winst.

20.7 Bij de berekening van de in het vorige lid bedoelde afrekening wordt steeds gecorrigeerd voor de voorzienbare en/of redelijkerwijs te verwachten herinzet van productiemiddelen door Leverancier.

20.8 Voor zover partijen over de hoogte van het in het vorige lid bedoelde bedrag geen overeenstemming weten te bereiken, wordt dit bedrag op basis van algemeen aanvaarde boekhoudkundige principes vastgesteld door een door beide partijen gezamenlijk te benoemen onafhankelijke en ter zake deskundige derde.

Ontbinding

20.9 Indien een partij tekortschiet in de nakoming van een overeengekomen verplichting, kan de andere partij haar in gebreke stellen waarbij de nalatige partij alsnog een redelijke termijn voor de nakoming wordt gegund. Blijft nakoming ook dan uit dan is de nalatige partij in verzuim. Ingebrekestelling is niet nodig wanneer voor de nakoming een fatale termijn geldt, nakoming blijvend onmogelijk is of indien uit een mededeling dan wel de houding van de andere partij moet worden afgeleid dat deze in de nakoming van haar verplichting zal tekortschieten.

20.10 Onverminderd hetgeen overigens in de Overeenkomst is vastgelegd, kan elk van de partijen de Overeenkomst door middel van een aangetekend schrijven buiten rechte geheel of gedeeltelijk ontbinden indien de andere partij in verzuim is dan wel een van de overige situaties bedoeld in artikel 20.9 zich voordoet.

20.11 Onverminderd hetgeen overigens in de Overeenkomst is bepaald, en onverminderd hetgeen overigens in de wet is bepaald, kan Opdrachtgever de Overeenkomst en alle daarmee samenhangende overeenkomsten middels een aangetekend schrijven ontbinden binnen twaalf (12) maanden nadat Opdrachtgever constateert dat:
i) Leverancier (voorlopige) surseance van betaling aanvraagt; of
ii) Leverancier zijn faillissement aanvraagt of in staat van faillissement wordt verklaard; of
iii) de onderneming van Leverancier wordt ontbonden; of

iv) Leverancier zijn onderneming staakt; of

v) sprake is van een ingrijpende wijziging in de zeggenschap over de activiteiten van de onderneming van Leverancier die maakt dat het in alle redelijkheid niet van de opdrachtgever kan worden verwacht dat zij de Overeenkomst in stand houdt; of

vi) op een aanmerkelijk deel van het vermogen van Leverancier beslag wordt gelegd (anders dan door Opdrachtgever); of

vii) het Bureau BIBOB een negatief advies heeft uitgebracht over de organisatie van Leverancier; of

viii) voor zover de Overeenkomst door middel van een aanbestedingsprocedure als bedoeld in de Aanbestedingswet tot stand is gekomen, zich gedurende de looptijd van de Overeenkomst ten aanzien van Leverancier uitsluitingsgronden voordoen als bedoeld in artikel 2.86 Aanbestedingswet.

20.12 Opdrachtgever kan de Overeenkomst en alle daarmee samenhangende overeenkomsten ook ontbinden indien hij op goede gronden aanneemt dat de rechter op een daartoe strekkende vordering op grond van de Aanbestedingswet de overeenkomst zal vernietigen. Leverancier heeft alsdan aanspraak op vergoeding van in redelijkheid voor de uitvoering van de Overeenkomst gemaakte kosten en in verband daarmee in redelijkheid voor de toekomst reeds aangegane verplichtingen. Indien Opdrachtgever echter aantoont dat de onrechtmatigheid (mede) aan Leverancier toerekenbaar is, komt Leverancier geen vergoeding toe.

20.13 Indien de overmachttoestand zestig (60) aaneengesloten dagen of gedurende in totaal meer dan negentig (90) dagen binnen een kalenderjaar heeft geduurd, of zodra duidelijk is dat de overmachttoestand langer dan dergelijke termijn zal duren, is de wederpartij van degene die zich op overmacht beroept, gerechtigd deze Overeenkomst tussentijds met onmiddellijke ingang (gedeeltelijk) te ontbinden.

Gevolgen van beëindiging

20.14 Leverancier retourneert of verwijdert bij het, op welke grond dan ook, eindigen van de Overeenkomst(en) onverwijld alle hem door Opdrachtgever ter hand gestelde documenten, boeken, bescheiden en andere zaken (waaronder begrepen gegevens- en informatiedragers). Bij vroegtijdige beëindiging geldt het voorgaande wederkerig.

Artikel 21. Controlerecht en medewerking audits bij Opdrachtgever

Controlerecht

21.1 Opdrachtgever is gerechtigd de naleving door Leverancier van de wezenlijke verplichtingen uit hoofde van de Overeenkomst, de GIBIT en de daarmee samenhangende overeenkomsten (SLA, bewerkersovereenkomst, etc.), alsmede de juistheid van toegezonden facturen, door een onafhankelijke ter zake deskundige derde te laten controleren.

21.2 De controle zal alleen plaatsvinden indien Opdrachtgever gerede twijfel heeft over de nakoming van de verplichtingen door Leverancier, of indien Opdrachtgever anderszins een gerechtvaardigd belang bij de controle heeft (o.m. wettelijke plicht, instructie toezichthouder).

21.3 Leverancier zal alle redelijkerwijs te verwachten medewerking verlenen aan een dergelijke controle. Leverancier zal in dat kader ten minste inzage verlenen in alle relevante gegevens en achtergrondinformatie die relevant kan zijn in het kader van voornoemde controle. Ook zal Leverancier toegang verlenen tot de locatie waar de diensten worden verleend.

21.4 Opdrachtgever staat er voor in dat de in het eerste lid bedoelde derde eventueel door Leverancier gehanteerde voorschriften zal opvolgen. Indien de controle niet (volledig) kan worden uitgevoerd vanwege voornoemde voorschriften, dan komt dit evenwel voor risico van Leverancier.

21.5 De kosten voor deze controle worden gedragen door Opdrachtgever (zowel eigen kosten als kosten van de Leverancier), tenzij de derde één of meer tekortkomingen van niet ondergeschikte aard van Leverancier constateert die ten nadele zijn van Opdrachtgever.

Medewerking audits bij Opdrachtgever

21.6 Voor zover Opdrachtgever afhankelijk is van Leverancier voor de uitvoering van (wettelijke verplichte) audits, zal Leverancier alle noodzakelijke medewerking verlenen aan de uitvoering van deze audits. De kosten voor deze medewerking worden gedragen door Opdrachtgever.

Artikel 22. Overstap van Opdrachtgever naar ander systeem, afschaling en overdracht

Exit-plan

22.1 Op eerste verzoek van Opdrachtgever zullen Partijen een exit-plan opstellen waarin wordt vastgelegd wat er dient te gebeuren ter voorbereiding op de in dit artikel beschreven werkzaamheden. Het exit-plan zal qua opbouw en mate van detaillering vergelijkbaar zijn met het Implementatieplan. Artikel 5.3 is van overeenkomstige toepassing op het opstellen van het exit-plan.

22.2 De in dit artikel bedoelde werkzaamheden zullen worden verricht overeenkomstig het exit-plan en het overig bepaalde in de GIBIT, tegen de dan reguliere tarieven van Leverancier.

Exit-scenario

22.3 Leverancier doet bij het, op welke grond ook beëindigen van de Overeenkomst(en), op eerste verzoek van Opdrachtgever datgene wat redelijkerwijs noodzakelijk is om er voor te zorgen dat een nieuwe leverancier of Opdrachtgever zelf zonder belemmeringen een soortgelijke ICT Prestatie ten behoeve van Opdrachtgever kan verrichten (zulks met uitzondering van de afgifte van de broncode van de Programmatuur).

22.4 Onder de in het vorige lid bedoelde redelijke maatregelen in het kader van de overstap naar een andere leverancier/ander systeem worden in ieder geval verstaan (naar keuze van Opdrachtgever):

i) het aanleveren van de in de ICT Prestatie opgeslagen gegevens conform de norm voor dataportabiliteit die deel uitmaakt van de Gemeentelijke ICT-kwaliteitsnormen;

ii) het aan Opdrachtgever aanleveren van de specifieke instellingen/inrichting van de ICT Prestatie (waaronder begrepen bedrijfsregels, macro's, etc.);

iii) het vernietigen van de gegevens waarvoor Opdrachtgever verantwoordelijk is (tegen afgifte van bewijs van vernietiging);

iv) het technisch ontvlechten en ontmantelen van (een deel van) de ICT Prestatie.

22.5 Leverancier verricht de in het vorige lid bedoelde werkzaamheden tegen de in de Overeenkomst bepaalde tarieven en condities of bij gebreke daarvan tegen de in het algemeen door Leverancier gehan-

teerde tarieven en nader overeen te komen condities. In afwijking van de vorige volzin worden voornoemde diensten kosteloos verricht indien sprake is van een toerekenbaar tekortschieten door Leverancier. De onder sub 22.4iii) bedoelde werkzaamheden worden op verzoek hoe dan ook kosteloos verricht.

Beperkte voorzetting van ICT Prestatie

22.6 Leverancier verklaart zich reeds nu voor alsdan bereid bij beeindiging van de Overeenkomst(en) – op welke grond dan ook – op eerste verzoek van Opdrachtgever:

i) Gebruiksrechten op de Programmatuur of soortgelijke programmatuur te verstrekken die Opdrachtgever in staat (blijven) stellen de met de Programmatuur opgeslagen gegevens te blijven raadplegen; en

ii) een beperkte vorm van Onderhoud te (blijven) verlenen op deze Programmatuur (namelijk binnen de kaders van de in het vorige lid bedoelde beperkte functionaliteit).

22.7 De duur en kosten voor de in het vorige lid bedoelde Gebruiksrechten en het daarmee samenhangende Onderhoud zullen in onderling overleg worden vastgesteld, met dien verstande dat:

i) de Gebruiksrechten en het daarmee samenhangende Onderhoud ten minste een zodanige duur kunnen hebben dat Opdrachtgever aan de wettelijke administratieplichten kan voldoen;

ii) de kosten voor de beperkte Gebruiksrechten en het beperkte Onderhoud in redelijke verhouding staan tot de oorspronkelijke kosten voor de gehele ICT Prestatie (naar rato van de verminderde functionaliteit).

22.8 Artikel 22.6 is niet van toepassing bij Hosting.

Overdracht ICT Prestatie

22.9 Opdrachtgever is gerechtigd de ICT Prestatie geheel of gedeeltelijk, inclusief alle daarbij behorende Gebruiksrechten en alle aanspraken in het kader van Onderhoud, onder gelijkblijvende voorwaarden over te dragen aan een gemeenschappelijke regeling of andere entiteit met een publieke functie in het kader van een uitbesteding van een deel van de activiteiten van Opdrachtgever. Leverancier zal alle noodzake-

lijke medewerking verlenen aan voornoemde overdracht. Leverancier is niet gerechtigd voor de overgang als zodanig kosten in rekening te brengen, wel voor eventueel aanvullend te verrichten werkzaamheden.

Verlengd gebruik

22.10 Leverancier verklaart zich voorts bereid om Opdrachtgever desgewenst toe te staan het gebruik van de ICT Prestatie na de beëindigingsdatum voor een redelijke periode te verlengen, indien de werkzaamheden overeenkomstig het Exit-plan niet tijdig zijn afgerond. Hiervoor zal een vergoeding in rekening worden gebracht, naar rato van de laatst geldende gebruiksvergoedingen, tenzij de niet-tijdige afronding van de Exit-werkzaamheden toerekenbaar is aan Leverancier (de verlenging is dan gratis). De onderhavige Overeenkomst blijft gedurende voornoemde verlenging onverminderd van kracht.

Artikel 23. Toepasselijk recht en geschillen

23.1 Op de Overeenkomst en alle daarmee verband houdende overeenkomsten, is uitsluitend Nederlands recht van toepassing.

23.2 De eenvormige wetten, opgesteld door de in 1964 te ‘s-Gravenhage gehouden diplomatieke Conferentie betreffende de unificatie van het internationale kooprecht (‘LUF’ en ‘LUVI’) en het Weens Koopverdrag, zijn niet van toepassing.

23.3 Alle geschillen (daaronder begrepen geschillen die slechts één van de partijen als zodanig beschouwt) die naar aanleiding van de Overeenkomst of daaruit voortvloeiende overeenkomsten tussen partijen mochten ontstaan, zullen aanhangig worden gemaakt bij de bevoegde rechter bij het arrondissement van Opdrachtgever.

II. Privacy, beveiliging en archivering

Voor zover met de ICT Prestatie (al dan niet door Leverancier) persoonsgegevens of andersoortige gegevens worden verwerkt die afkomstig zijn van Opdrachtgever of waarvoor Opdrachtgever verantwoordelijk is, gelden in aanvulling op het algemene deel de bepalingen uit het onderhavige hoofdstuk.

Artikel 24. Bewerkersrelatie

24.1 Voor zover Leverancier in het kader van de uitvoering van de Overeen-

komst persoonsgegevens voor Opdrachtgever verwerkt, wordt Leverancier als bewerker / verwerker in de zin van de Wet bescherming persoonsgegevens (Wbp) / EU verordening 2016/679 (AVG) aangemerkt.

24.2 De Overeenkomst in combinatie met de GIBIT wordt door partijen aangemerkt als overeenkomst in de zin van artikel 14 lid 2 Wbp / artikel 28 AVG.

24.3 Leverancier verklaart zich reeds nu voor alsdan bereid een separate bewerkersovereenkomst af te sluiten met Opdrachtgever met daarin opgenomen aanvullende of afwijkende afspraken omtrent de verwerking van persoonsgegevens. De betreffende bewerkersovereenkomst prevaleert op hetgeen in de onderhavige voorwaarden is bepaald.

24.4 Opdrachtgever stemt er reeds nu voor alsdan mee in dat Leverancier de verwerking van persoonsgegevens kan uitbesteden aan een derde (een zogenaamde 'sub-bewerker') , mits Leverancier:

i) louter sub-bewerkers betrekt die afdoende garanties bieden met betrekking tot het toepassen van passende technische en organisatorische maatregelen opdat de verwerking aan de vereisten van de wet- en regelgeving voldoet en de bescherming van de rechten van de betrokkene is gewaarborgd;

ii) de volledige aansprakelijkheid aanvaardt voor het handelen van de ingeschakelde sub-bewerkers;

iii) met deze sub-bewerker voorafgaand aan de uitbesteding een schriftelijke overeenkomst sluit, op grond waarvan:

(1) alle verplichtingen die op grond van de Overeenkomst (waaronder de GIBIT) met betrekking tot de verwerking van persoonsgegevens op Leverancier rusten mede komen te rusten op deze sub-bewerker;

(2) de betreffende sub-bewerker zich eveneens richt naar de instructies van Opdrachtgever.

Artikel 25. Verwerking persoonsgegevens

25.1 Begrippen uit de Wbp / AVG die in dit hoofdstuk zijn overgenomen hebben dezelfde betekenis als in de Wbp / AVG gedefinieerd.

25.2 Leverancier is niet gerechtigd om op enig moment de persoonsgegevens die zij ter beschikking krijgt op enigerlei wijze geheel of gedeeltelijk anders te (doen) gebruiken dan voor de uitvoering van de Overeen-

komst, een en ander behoudens afwijkende wettelijke verplichtingen.

25.3 Leverancier zal, onverminderd hetgeen in artikel 26 staat vermeld, passende technische en organisatorische beveiligingsmaatregelen treffen om de persoonsgegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking. Deze maatregelen garanderen, rekening houdend met de stand van de techniek en de kosten van de tenuitvoerlegging daarvan, een passend beveiligingsniveau gelet op de risico's die de verwerking en de aard van de te beschermen gegevens meebrengen. De maatregelen zijn er mede op gericht onnodige verzameling en verdere verwerking van persoonsgegevens te voorkomen.

25.4 Leverancier legt ten minste een algemene beschrijving van de in het vorige lid bedoelde getroffen technische en organisatorische beveiligingsmaatregelen schriftelijk vast.

25.5 Leverancier verwerkt persoonsgegevens op behoorlijke en zorgvuldige wijze en in overeenstemming met de toepasselijke wet- en regelgeving, de instructies van Opdrachtgever alsmede een eventueel toepasselijke gedragscode van Opdrachtgever.

25.6 Leverancier verwerkt persoonsgegevens louter binnen de Europese Economische Ruimte, althans een land dat door een besluit van de Europese Commissie als veilig is aangemerkt, tenzij uitdrukkelijk anders overeengekomen.

25.7 Alle persoonsgegevens worden als vertrouwelijk in de zin van artikel 15 aangemerkt.

25.8 Het controlerecht van artikel 21 is van overeenkomstige toepassing.

25.9 Leverancier onderhoudt zelf geen contact met de betrokkene. Indien de betrokkene Leverancier benadert, zal hij deze verwijzen naar Opdrachtgever. Indien Opdrachtgever (bijv. om technische redenen) niet zelf (volledig) gehoor kan geven aan de uitoefening van een recht door betrokkene (o.m. inzage, correctie, verzet), dan zal Leverancier daar op verzoek zo spoedig mogelijk alle noodzakelijke medewerking aan verlenen.

Artikel 26. Informatiebeveiliging

26.1 Leverancier staat er voor in dat met de ICT Prestatie door Opdrachtgever kan worden voldaan aan de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG) welke deel uitmaakt van de Gemeentelijke

ICT-kwaliteitsnormen (voor zover relevant voor de ICT Prestatie), althans een andere overeengekomen norm voor informatiebeveiliging.

26.2 Indien de ICT Prestatie (gedeeltelijk) door Leverancier beheerd wordt (bijv. bij Hosting), of dienstverlening betreft die door Leverancier verricht wordt, staat Leverancier er (voor dat deel) voor in dat de ICT Prestatie voldoet aan de in lid 1 bedoelde norm voor informatiebeveiliging, althans een andere overeengekomen norm. Artikel 25.4 is van overeenkomstige toepassing.

26.3 Leverancier staat er voor in dat al het door hem ingeschakelde personeel en andere derden zullen werken overeenkomstig de overeengekomen normen voor informatiebeveiliging.

26.4 Informatie over de getroffen beveiligingsmaatregelen wordt als vertrouwelijke informatie als bedoeld in artikel 15 beschouwd.

Artikel 27. Meldplicht beveiligingsincidenten

27.1 Leverancier zal Opdrachtgever na ontdekking onverwijld informeren over alle inbreuken op de beveiliging alsmede andere incidenten die op grond van wetgeving moeten worden gemeld aan een toezichthouder of betrokkene, onverminderd de verplichting de gevolgen van dergelijke inbreuken en incidenten zo snel mogelijk ongedaan te maken dan wel te beperken.

27.2 Leverancier zal het doen van meldingen aan de toezichthouder(s) overlaten aan Opdrachtgever (behoudens dwingendrechtelijke verplichtingen).

27.3 Leverancier zal alle noodzakelijke medewerking verlenen aan het zo nodig, op de kortst mogelijke termijn, verschaffen van aanvullende informatie aan de toezichthouder(s) en/of betrokkene(n).

27.4 De kosten voor de werkzaamheden die op grond van dit artikel door Leverancier moeten worden verricht komen voor rekening van Leverancier, tenzij Leverancier bewijst dat de inbreuk niet aan hem is toe te rekenen.

27.5 Leverancier houdt een gedetailleerd logboek bij van alle inbreuken op de beveiliging, evenals de maatregelen die in vervolg op dergelijke inbreuken zijn genomen.

27.6 Leverancier geeft op eerste verzoek van Opdrachtgever inzage in het in het vorige lid bedoelde logboek.

27.7 Indien Leverancier toerekenbaar in strijd handelt met een van deze verplichtingen van dit artikel zal Leverancier onmiddellijk – dus zonder

dat daarvoor nog een ingebrekestelling moet worden verstuurd - aansprakelijk zijn voor alle schade die Opdrachtgever als gevolg daarvan lijdt, waaronder begrepen eventueel door Opdrachtgever te verbeuren boetes (binnen de kaders van artikel 13). De boetebepaling van artikel 15.4 is van overeenkomstige toepassing.

27.8 De verplichtingen in dit artikel (behoudens artikel 27.5) zijn niet van toepassing indien en voor zover de inbreuken/incidenten geen enkel risico vormen voor de gegevens die afkomstig zijn van Opdrachtgever of waarvoor Opdrachtgever verantwoordelijk(e) is.

Artikel 28. Archivering

28.1 Tenzij in de Overeenkomst anders bepaald dient Leverancier zorg te dragen voor het aantoonbaar beheren en beschermen van beheerde gegevens door beveiligingsmaatregelen, preserveringsmaatregelen en controles ten aanzien van archivering, conform de vereisten die deel uitmaken van de Gemeentelijke ICT-kwaliteitsnormen.

28.2 Leverancier dient zich aantoonbaar aan de in de Gemeentelijke ICT-kwaliteitsnormen althans de Overeenkomst gestelde bewaartermijnen te houden en pas over te gaan tot verwijdering na toestemming van Opdrachtgever.

28.3 Leverancier moet archiefbescheiden kunnen migreren naar archiefsystemen van Opdrachtgever conform de vereisten die deel uitmaken van de Gemeentelijke ICT-kwaliteitsnormen. Leverancier verricht de werkzaamheden voor het daadwerkelijk migreren van archiefbescheiden tegen de in de Overeenkomst bepaalde tarieven en condities of bij gebreke daarvan tegen de in het algemeen door Leverancier gehanteerde tarieven en nader overeen te komen condities.

28.4 Indien op het moment van opschorting, opzegging of ontbinding van de Overeenkomst Leverancier archiefbescheiden van Opdrachtgever onder zich heeft die vanwege de plaatsing en inrichting van de ICT Prestatie niet tevens berusten onder de Opdrachtgever als zorgdrager, dan verplicht Leverancier zich te handelen als zou hij een kennisgeving hebben ontvangen onder artikel 11 lid 1 Archiefwet 1995 (ongeacht of de betreffende archiefbescheiden zijn opgenomen in Derdenprogrammatuur).

III. Hosting

Het bepaalde in het onderhavige hoofdstuk is, in aanvulling op het algemene hoofdstuk, alsmede hoofstuk II, van toepassing indien en voor zover de ICT Prestatie (mede) Hosting betreffen (zoals bij ASP, Cloud, IAAS, etc.).

Artikel 29. Algemeen

29.1 Leverancier zal alle noodzakelijke gegevens, zoals URLs en inloggegevens, aan Opdrachtgever ter beschikking stellen die noodzakelijk zijn om daadwerkelijk gebruik te kunnen maken van de ICT Prestatie.

29.2 Leverancier is niet gerechtigd de Hosting op te schorten, behalve voor zover voortzetting niet gevergd kan worden. De enkele eenmalige niet-betaling rechtvaardigt dit niet.

Artikel 30. Opgeslagen gegevens

30.1 Opdrachtgever is zelf te allen tijde volledig verantwoordelijk voor het gebruik dat zij maakt van de Hosting en voor de gegevens die zij met behulp van de Hosting opslaat, opvraagt, verspreidt en anderszins gebruikt.

30.2 Indien en voor zover er aanwijzigingen of vermoedens bestaan dat de middels de Hosting verwerkte gegevens onrechtmatig jegens derden zijn, zal Leverancier Opdrachtgever daarover zo spoedig mogelijk informeren.

30.3 Leverancier zal de betreffende gegevens niet zonder voorafgaand overleg met Opdrachtgever verwijderen, tenzij de gegevens zodanig evident onrechtmatig zijn en de spoedeisendheid van het geval maakt dat voorafgaand overleg met Opdrachtgever niet kan worden afgewacht.

Artikel 31. Onderhoud en Beschikbaarheid

31.1 Vanaf het moment van Acceptatie van de ICT Prestatie zijn de specifieke afspraken omtrent het Onderhoud (ook) op de Hosting van toepassing (zoals de gegarandeerde service-levels en de overeengekomen Beschikbaarheid).

31.2 Indien en voor zover in de Overeenkomst geen Service Levels ten aanzien van de Beschikbaarheid van de Hosting zijn afgesproken, geldt een Service Level van 98% Beschikbaarheid per maand op werkdagen tussen 08.00-18.00uur.

31.3 Leverancier verzorgt – in afwijking van het bepaalde in artikel 8.10 – bij Hosting de installatie van Updates en Upgrades.

31.4 Het recht om de ingebruikname van Updates en/of Upgrades te weigeren als bedoeld in artikel 8.11 is niet van toepassing bij generieke Hosting die door Leverancier aan meerdere klanten wordt aangeboden, tenzij in de Overeenkomst anders is bepaald.

Artikel 32. Waarborgen continuiteit

32.1 Gelet op de grote afhankelijkheid van Leverancier alsmede het continuiteitsrisico bij incidenten en calamiteiten (zoals faillissement) die er bij Hosting bestaat, verklaart Leverancier zich reeds nu voor alsdan bereid aanvullende afspraken met Opdrachtgever te maken teneinde voornoemde risico's te verkleinen.

32.2 De in het vorige lid bedoelde aanvullende afspraken kunnen onder meer bestaan uit:

i) het maken van afspraken over het periodiek terug of aan een derde partij leveren van de door Leverancier verwerkte gegevens ('data-escrow'); en/of

ii) het met een derde partij sluiten van een overeenkomst die ertoe strekt dat de betreffende derde partij zich hoofdelijk verbindt tot of borg staat voor de nakoming van de Overeenkomst; en/of

iii) het met een derde partij sluiten van een (tri-partite) overeenkomst die ertoe strekt dat de betreffende derde partij (voortdurend) over alle benodigde gegevens komt te beschikken om in voorkomend geval (een deel van) de ICT Prestatie uit de Overeenkomst – al dan niet op basis van een nieuwe overeenkomst – in plaats van Leverancier te kunnen (gaan) verrichten.

IV Artikelgewijze toelichting

I. Algemeen deel

Artikel 1. Begrippen

In dit artikel zijn de diverse centrale begrippen uit de GIBIT gedefinieerd. Deze begrippen worden niet afzonderlijk toegelicht, doch worden besproken bij de verschillende artikelen waar ze worden gebruikt.

Artikel 2. Toepasselijkheid

Dit artikel geeft enkele algemene regels omtrent de toepasselijkheid van de GIBIT. Daarbij wordt onder ICT Prestatie verstaan de totale leveringsomvang van te leveren producten en diensten en gebruiksrechten.

Artikel 2.1 bepaalt dat de GIBIT niet alleen van toepassing is op de ICT Prestaties uit de Overeenkomst, maar ook op daarmee – eventueel in de toekomst overeen te komen – samenhangende ICT Prestaties. Hiermee wordt beoogd te voorkomen dat op latere, aanvullende, overeenkomsten opeens een andere set voorwaarden van toepassing zou zijn. **Let wel:** er is niet beoogd leveranciers voor *alle* toekomstige opdrachten bij voorbaat aan de GIBIT te binden. Het beding heeft alleen betrekking op overeenkomsten die samenhangen met een overeenkomst waarbij de toepasselijkheid van de GIBIT reeds bedongen is. Een voorbeeld is dat op een later moment alsnog een onderhoudsovereenkomst wordt afgesloten terwijl die oorspronkelijk niet tot de overeenkomst behoorde. Deze betreffende onderhoudsovereenkomst valt dan onder de voorwaarden van de GIBIT. Gemeenten dienen er dus op

bedacht te zijn voorafgaand aan het sluiten van een overeenkomst – dus al in de fase van een offerteaanvraag/aanbesteding – de GIBIT van toepassing te verklaren. Zodoende wordt geborgd dat vanaf het begin de GIBIT als voorwaarden gelden, ook voor aanvullende overeenkomsten die op een later moment worden afgesloten.

Artikel 2.2 ziet op de indeling van de GIBIT in drie hoofdstukken. Het algemene hoofdstuk I is altijd van toepassing; de overige hoofdstukken met bepalingen over privacy, beveiliging, archiefbeheer en hosting zijn van toepassing naar gelang de aard van de te leveren producten/diensten.

Artikel 2.3 is opgenomen om algemene voorwaarden van leveranciers van de hand te wijzen. Doel van deze bepaling is te voorkomen dat de GIBIT niet van toepassing is in het geval leveranciers eigen voorwaarden van toepassing verklaren. De bepaling hangt samen met het bepaalde in artikel 6:225 lid 3 BW. Daarin staat – in de kern – dat de algemene voorwaarden die als eerste van toepassing zijn verklaard van toepassing blijven, tenzij bij het van toepassing verklaren van een tweede set algemene voorwaarden de eerste set *uitdrukkelijk* van de hand is gewezen. Het is overigens de vraag of het bepaalde in dit artikel voldoet aan het uitdrukkelijkheidsvereiste als bedoeld in artikel 6:225 lid 3 BW. Gemeenten dienen er dus altijd alert op te zijn dat leveranciers in het aanbod geen eigen voorwaarden van toepassing verklaren.

Artikel 2.4 is opgenomen om bij eventuele ongeldigheid van een bepaling uit de GIBIT:

1. te voorkomen dat dit effect heeft op de overige bepalingen van de GIBIT; en
2. partijen te verplichten nieuwe afspraken te maken waarbij doel en strekking van de oorspronkelijke bepaling in acht worden genomen.

Artikel 2.5 bepaalt dat de overeenkomst prevaleert op hetgeen in de GIBIT is bepaald. Het is een zeer belangrijke bepaling. Dit hangt samen met het abstracte karakter van de GIBIT en het feit dat de GIBIT een vangnet is. Voor de goede orde: in de overeenkomst tussen gemeente en leverancier kan van iedere bepaling in de GIBIT worden afgeweken. Dat in de GIBIT bij sommige bepalingen uitdrukkelijk wordt verwezen naar de overeenkomst en in andere

bepalingen niet, is hiervoor niet relevant. De verwijzingen naar de overeenkomst zijn in voorkomend geval louter opgenomen om extra aandacht te vestigen op de mogelijkheid om af te wijken.

Artikel 2.6 bepaalt ten slotte dat wijzigingen op de GIBIT schriftelijk overeengekomen moeten zijn. Ook is bepaald dat wijzigingen slechts voor de in artikel 2.1 bedoelde overeenkomst gelden. De gedachte is dat voor ieder project opnieuw moet worden bezien welke bepalingen al dan niet relevant zijn.

Artikel 3. Totstandkoming overeenkomst

In dit artikel komt de zorgplicht van de leverancier duidelijk naar voren. Deze zorgplicht voor leveranciers geldt hoe dan ook op grond van de wet en de rechtspraak. Vaak is echter niet duidelijk wat precies onder deze abstracte zorgplicht wordt verstaan. Die wordt daarom hier in **artikel 3** nader beschreven.

De GIBIT vult deze zorgplicht in ieder geval voor wat betreft de voorfase van contracteren nader in. De leverancier moet zich namelijk niet alleen goed op de hoogte stellen van relevante informatie over opdrachtgever en het voorgenomen project (**artikel 3.2/3.3**), maar daar vervolgens ook wat mee doen door deze informatie te vertalen in het aanbod en de risicoanalyse (**artikel 3.4/3.5**). Van de leverancier wordt in feite verwacht dat hij voldoet aan het ‘ken uw klant’ en ‘ken uw product’ principe. Doordat de leverancier de gemeente moet waarschuwen voor eventueel gesignaleerde risico’s, wordt bovendien bewerkstelligd dat de gemeente vooraf weet met welke risico’s rekening gehouden moet worden.

De gedachte is dat de inventarisatie van risico’s zo meer naar voren wordt gehaald en beide partijen beter weten waar ze aan beginnen en vroegtijdig maatregelen kunnen treffen.

De aard en omvang van de risicoanalyse zal per opdracht verschillen. Bij kleine opdrachten of projecten is denkbaar dat de inventarisatie nauwelijks iets om het lijf heeft; bij grote opdrachten en projecten zal hier meer van beide partijen gevergd worden. Het is niet per se noodzakelijk dat er onderzoek bij de gemeente op locatie plaatsvindt. Een leverancier die zijn eigen product kent en ervaring heeft met het implementeren daarvan, weet welke informa-

tie vereist is voor het kunnen doen van een goed aanbod en welke valkuilen in dat aanbod dienen te worden geadresseerd (althans behoort dit te weten). Bij zeer risicovolle en complexe projecten ligt het voor de hand separaat advies in te winnen over de risico's. Dit kan ook mogelijk als afzonderlijke (deel) opdracht worden ingewonnen.

Afhankelijk van de waarde van de opdracht en/of het eigen beleid van gemeenten kan het zijn dat een opdracht aanbesteed wordt. De aanbestedingswetgeving beperkt de ruimte voor leveranciers om zelf bij de gemeenten tijdens het aanbestedingsproces navraag te doen. Dit wordt erkend in **artikel 3.6** van de GIBIT.

In **artikel 3.7** wordt voor wat betreft zogenaamde Derdenprogrammatuur vooruit verwezen naar artikel 19. De GIBIT erkent hiermee dat leveranciers soms zelf ook gebonden zijn aan bepaalde voorwaarden en mogelijkheden die hen beperken in de vrijheid een volledig eigen aanbod te doen. Meer over Derdenprogrammatuur bij de betreffende toelichting.

Met '*schriftelijk*' in **artikel 3.8** is wordt bedoeld '*geschreven*', niet '*op papier*'. Elektronische communicatie is dus ook toegestaan.

Artikel 4. Uitvoering overeenkomst

In **artikel 4.1** is opgenomen dat termijnen fataal zijn. Een fatale termijn wil zeggen dat bij overschrijding daarvan de leverancier automatisch, zonder nadere ingebrekestelling door gemeente, in verzuim raakt. Bij overschrijding van een termijn kan de gemeente de overeenkomst direct ontbinden en/of schade verhalen.

Let op: Daar wordt in artikel 5.6 voor wat betreft de implementatie alweer van afgeweken. Ook wordt het fatale karakter gerelativeerd door het bepaalde in artikel 4.4 (zie hierna).

Artikel 4.2 biedt de ruimte om de in artikel 3 bedoelde risicoanalyse op een later moment uit te voeren. Dit geeft leveranciers de ruimte om niet al in de offertefase veel energie in de risicoanalyse te hoeven steken. Het risico dat in deze latere fase opeens onacceptabele risico's naar voren komen, wordt

afgedekt door het recht van de gemeente om in die situatie (tegen vergoeding van kosten) de overeenkomst te ontbinden. Leveranciers hebben dit recht niet. Hier is expliciet voor gekozen: immers, van een leverancier mag verwacht worden dat hij reeds bij de eerste aanbieding (voordat de risicoanalyse is uitgevoerd) goed in beeld heeft wat de risico's aan zijn kant zijn ten aanzien van het leveren van de ICT Prestatie.

Artikel 4.3 bepaalt dat indien het transport (in opdracht van of) door de leverancier wordt verzorgd, het transportrisico bij de leverancier ligt, tenzij anders overeengekomen.

In **artikel 4.4** is uitdrukkelijk bepaald dat de gemeente alle verplichtingen die uit de overeenkomst voortvloeien zal naleven. Strikt genomen is de bepaling overbodig, omdat dit ook al uit de wet en de overeenkomst voortvloeit.
De bepaling heeft vooral een belangrijke signaalfunctie, zowel richting gemeenten als leveranciers. Voor gemeenten is van belang dat zij zich terdege realiseren dat het van belang is dat de – bijvoorbeeld in het Implementatieplan – gemaakte afspraken over de te verrichten werkzaamheden ook (tijdig) worden nagekomen. Voor leveranciers geldt dat indien fatale termijnen (zie artikel 4.1) niet gehaald kunnen worden door toedoen van de gemeenten, de gemeente aldus geen beroep toekomt op het fatale karakter van de betreffende termijnen.

Artikel 5. Implementatie ICT Prestatie

De GIBIT gaat ervan uit dat de leverancier de implementatie verzorgt. De implementatie is daarbij bewust ruim gedefinieerd (zie artikel 1.15) en gaat uit van het beheerst en projectmatig inrichten en in gebruik nemen van de ICT Prestatie in de organisatie en het inpassen ervan binnen de bestaande informatievoorziening. Dit laatste uiteraard binnen de kaders van het Overeengekomen gebruik. De implementatie leidt dus niet tot wijzigingen van de gemaakte afspraken over de te leveren functionaliteit.

In artikel 5 komt het vroegtijdig adresseren van risico's aan de orde. **Artikel 5.1** bepaalt dat de implementatie overeenkomstig het implementatieplan plaatsvindt en **artikel 5.2** bepaalt dat het opstellen van een dergelijk plan altijd verlangd kan worden. **Artikel 5.3** geeft bovendien aan welke onderwer-

pen in een dergelijk plan opgenomen moeten worden. Het idee is dat het in belang van beide partijen is vooraf – en niet pas gaandeweg het project – goed na te denken over al datgene dat noodzakelijk is om de implementatie tot een succes te maken. Overigens zullen in de praktijk niet alle in het artikel 5.3 genoemde onderwerpen voor ieder project van belang zijn.

In **artikel 5.4** komt de in artikel 3 en 4 bedoelde risicoanalyse terug. Hierin is opgenomen dat aanpassingen aan het Applicatielandschap van de gemeente die noodzakelijk zijn maar vooraf niet-voorzien waren, doch gelet op de zorgplicht van leverancier achteraf wel voorzienbaar waren geweest, voor rekening van de leverancier komen. Het artikel vormt in zoverre de '*proof of the pudding*' van (de kwaliteit van) de eerder genoemde risicoanalyse ten aanzien van de inpasbaarheid van de aangeboden oplossing bij de gemeente. Het artikel is alleen van toepassing op aanpassingen aan het Applicatielandschap die de Leverancier had kunnen of behoren te voorzien. Het artikel probeert in zoverre te voorkomen dat leveranciers die willens en wetens een onvolledig of ondoordacht aanbod doen bij de gunning voordeel halen en later 'beloond' worden met meerwerkopdrachten.

Het artikel is bovendien alleen van toepassing op aanpassingen aan het Applicatielandschap die voor de Implementatie (en daarmee dus voor het Overeengekomen gebruik) noodzakelijk zijn. Het artikel vormt dus ook zeker geen vrijbrief voor gemeenten om op kosten van leveranciers allerlei niet aan de Implementatie gerelateerde onderdelen van het Applicatielandschap te laten upgraden, of om verderstrekkende verbeteringen te verlangen dan die noodzakelijk zijn voor de Implementatie. Voor verdergaande aanpassingen maakt de gemeente nieuwe/separate afspraken. Indien in de praktijk blijkt dat het voor gemeenten aantrekkelijk is om bij de aanpassing in het Applicatielandschap verder te gaan dan het voor de Overeenkomst strikt noodzakelijke, dan ligt het voor de hand dat partijen daarover separate afspraken maken (bijv. een afzonderlijk upgrade project met een korting op grond van artikel 5.4).

Artikel 5.5 erkent dat gedurende de implementatie werkzaamheden nog wel eens willen schuiven. Tussentijdse opleverdata zijn daarom niet fataal. De eindtermijn is uitdrukkelijk wel fataal. Dit in de gedachte dat uiteindelijk het

eindresultaat voor de gemeente telt: een functionerende ICT Prestatie op de overeengekomen datum. De weg ernaartoe is over het algemeen daarbij van minder zwaar gewicht.

Artikel 5.6 ziet op de bereidheid van de leverancier om later alsnog of nogmaals aan de implementatie gerelateerde werkzaamheden te verrichten. Te denken valt hierbij aan een na inbedrijfsstelling of livegang alsnog uit te voeren conversie, het na livegang alsnog aanleggen van extra koppelingen of het na livegang alsnog verzorgen van (aanvullende) trainingen. Dergelijke werkzaamheden worden in beginsel uitgevoerd binnen hetzelfde kader van artikel 5 (dus ook een plan, alleen einddatum is fataal, etc.). Leverancier is uiteraard gerechtigd voor dit meerwerk kosten in rekening te brengen. Dat gebeurt overeenkomstig de (geïndexeerde) overeengekomen dan wel gebruikelijke tarieven.

Artikel 6. Gemeentelijke ICT-kwaliteitsnormen, Interoperabiliteitseisen en standaarden

Een van de doelen van de GIBIT is te komen tot een hogere kwaliteit van de informatievoorziening van gemeenten en van de ICT-producten en diensten die daar deel van uitmaken. Ook wenst de GIBIT gestandaardiseerde gegevensuitwisseling te stimuleren zodat informatie goed, veilig en betrouwbaar gedeeld kan worden en processen ketengericht kunnen worden uitgevoerd. Dit komt terug in **artikel 6**.

Artikel 6 schrijft voor dat de ICT Prestatie moet voldoen aan de Gemeentelijke ICT-kwaliteitsnormen. KING geeft aan voor bepaalde soorten/typen applicaties of ICT-producten/diensten welke normen gelden. Het verplichtende karakter van die normen komt terug in **artikel 6.1** onder i. Deze set van verplichte normen en standaarden wordt periodiek door VNG/KING gepubliceerd. Binnen de set vallen alleen normen en standaarden die verplicht zijn binnen het werkingsgebied van gemeenten, van gemeentelijke samenwerkingsverbanden of voor ketens waarin gemeenten opereren. Het betreft open standaarden en normen waarbij leveranciers bij de vaststelling zijn betrokken.

Verplicht zijn normen en standaarden die een wettelijk kader hebben en standaarden op de lijst van open standaarden zoals vastgesteld en gepubliceerd door het bureau Forum Standaardisatie (ook wel de gangbare standaarden

en/of standaarden op de pas-toe-of-leg-uit lijst) en standaarden die als landelijke gemeentelijke standaard of norm door VNG/KING zijn vastgesteld. Het betreft normen en standaarden die de volgende ICT-kwaliteitsgebieden afdekken (tussen haakjes staan ter verduidelijking voorbeelden van betreffende normen en standaarden):

- Architectuur (GEMMA);
- Interoperabiliteit (NEN3610, StUF, SUWIML, Digikoppeling, iWMO);
- Beveiliging (Baseline Informatiebeveiliging Gemeenten);
- Dataportabiliteit;
- Metadatering (TMLO);
- Toegankelijkheid (Webrichtlijnen);
- Archivering (NEN-ISO 15489-1 NL);
- Infrastructuur (Generieke Digitale Infrastructuur, aansluiten op Stelsel van Basisregistraties);
- Documentatie;
- E-facturering.

Standaarden of versies van standaarden die nog in ontwikkeling zijn, vallen buiten de GIBIT. De standaarden en/of nieuwe versies dienen formeel te zijn vastgesteld en een status te hebben van 'in gebruik' of een soortgelijke betekenis. De set van toe te passen normen zal op www.gibit.nl worden vermeld. **Artikel 6.1** onder ii geeft de gemeente de ruimte om ook aan andere normen als eis op te nemen. Deze eisen dienen dan in bijvoorbeeld een Programma van Eisen of offerteaanvraag gespecificeerd te worden.

Veel normen en standaarden schrijven voor dat bepaalde preventieve testen worden uitgevoerd zodat aangetoond wordt dat aan de betreffende norm wordt voldaan. **Artikel 6.2** bepaalt dat deze testen moeten worden uitgevoerd voorafgaand aan de implementatie en op een omgeving van de leverancier. De gedachte is dat het tot een goed ontwikkelproces behoort dat de leverancier zijn eigen product grondig test op de kwaliteitsaspecten (o.a. technische inpasbaarheid en interoperabiliteit) die voor de klant niet goed te beoordelen zijn, alvorens het product aan klanten ter beschikking te stellen. Tevens bepaald artikel 6.2 dat de leverancier moet aantonen dat de ICT Prestatie aan de normen voldoet middels het overleggen van een positief testrapport. Op grond van **artikel 6.3** is het opnieuw preventief testen niet noodzake-

lijk indien de testen onder vergelijkbare omstandigheden op de dezelfde versie van het product, van de norm en van de testset al eens succesvol zijn doorlopen. Dit maakt dat het artikel over de preventieve testen met name bij nieuwe producten, nieuwe versies van producten of producten die nog niet in een vergelijkbare context zijn gebruikt relevant is.

Artikel 6.4 benoemt (volledigheidshalve) dat gedurende de Acceptatie-procedure wordt getoetst in hoeverre de ICT Prestatie aan de normen voldoet. Strikt genomen volgt dit al uit het gegeven dat het voldoen aan de normen tot het 'Overeengekomen gebruik' hoort.

Artikel 6.5 bepaalt dat eventuele koppelingen met andere systemen gedurende de Acceptatieprocedure moeten worden getest op correcte interoperabiliteit. Veel applicaties werken immers alleen goed in de context van koppelingen met andere applicaties. Dat is voor de eindgebruiker echter vaak niet goed zichtbaar, maar wel essentieel voor veilige en betrouwbare informatieketens.

In **artikel 6.6** is bepaald dat in beginsel de gemeente verantwoordelijk is om tijdig de leveranciers van de andere relevante applicaties bij de ketentest te betrekken (zij is immers de partij met de contractuele relatie). De leverancier verzorgt in beginsel de coördinatie tussen alle bij de ketentest betrokken partijen. De leverancier zal immers veelal de expertise in huis hebben om dit proces het best te kunnen begeleiden.

In **artikel 6.7** is een regeling opgenomen voor het geval de ketentest niet slaagt. Het artikel maakt onderscheid tussen twee situaties:

1. Het falen van de test is toerekenbaar aan Leverancier. Deze situatie doet zich bijvoorbeeld voor indien de door leverancier geleverde ICT Prestatie (zoals een Koppeling) gebrekkig is. In dat geval gaat eenvoudigweg de hoofdregel van de Acceptatieprocedure op (zie artikel 7, althans de afspraken in de overeenkomst omtrent acceptatie);
2. Het falen van de test is niet toerekenbaar aan Leverancier. Deze situatie doet zich bijvoorbeeld voor indien er gebreken blijken te zitten in de programmatuur van de andere – tevens bij de ketentest betrokken – leveranciers (waarmee de ICT Prestatie gekoppeld

wordt). Leverancier is niet bij de levering van die programmatuur betrokken en het gebrek is dan ook (uiteraard) niet aan leverancier toerekenbaar. Dat laat onverlet dat het voor de gemeente wel noodzakelijk is dat er een oplossing gevonden wordt. Voor de gemeente is immers een functionerende keten van belang. Vandaar de bepaling dat de acceptatieprocedure in dat geval wordt opgeschort totdat partijen een acceptabele oplossing hebben weten te bereiken. Het is denkbaar en zelfs waarschijnlijk dat die oplossing in feite meerwerk omvat. Omvat die oplossing inderdaad meerwerk, dan mag dit alleen worden uitgevoerd na uitdrukkelijke instemming/opdracht van de gemeente. Uiteraard is denkbaar dat in de praktijk ineens zowel het nieuwe/bijgestelde plan, als het (daarin beschreven en daarmee) uit te voeren meerwerk door de gemeente wordt goedgekeurd.

De GIBIT kiest hiermee uitdrukkelijk voor een meer 'holistische' benadering van het Applicatielandschap van de gemeente. De gemeente wil immers dat de verschillende applicaties goed samenwerken. Doordat de GIBIT eveneens eisen dat ICT Prestaties aan standaarden voldoen, is de verwachting dat op termijn, zeker zodra er door meer leveranciers onder toepasselijkheid van de GIBIT wordt geleverd, veelvoorkomende problemen en knelpunten bij koppelingen worden gereduceerd en het functioneren van proces- en informatieketens beter is geborgd.

Artikel 7. Acceptatie

In **artikel 7** is de acceptatieprocedure beschreven.

Het is in het belang van beide partijen dat vooraf helder is op welke wijze de acceptatieprocedure zal verlopen. Vandaar ook dat reeds in artikel 5.3 sub viii is bepaald dat, als onderdeel van het Implementatieplan, moet worden vastgelegd op welke wijze de acceptatieprocedure wordt uitgevoerd. Er zal echter niet altijd een implementatieplan zijn. Ook is denkbaar dat het implementatieplan ten aanzien van de acceptatietest geen of onvoldoende uitgewerkte afspraken bevat. Vandaar dat **artikel 7.1** bepaalt dat op verzoek van de gemeente alsnog een schriftelijk testprotocol wordt opgesteld. De verwijzing naar artikel 5.2 is bedoeld om aan te geven dat de leverancier

penvoerder is van het plan (als meest deskundige) en voor het opstellen van het plan geen afzonderlijke vergoeding in rekening mag brengen.

De overige bepalingen van artikel 7 moeten worden gezien zijn 'vangnetbepalingen'. Deze artikelen geven de kaders voor zover er in de Overeenkomst of in een ander bovenliggend document geen meer specifieke afspraken over de Acceptatieprocedure zijn gemaakt. Het geheel van deze bepalingen beschrijft de Acceptatieprocedure.

Artikel 7.2 geeft in de kern aan wat er tijdens testen gebeurt. We lichten de elementen puntsgewijs toe:

- Er wordt getest op Gebreken (zie artikel 1.9), dus op het niet voldoen aan het *Overeengekomen gebruik* (zie artikel 1.23). Er wordt uitdrukkelijk niet getest op aspecten van de ICT Prestatie die niet overeengekomen zijn (dat zou immers ook niet toerekenbaar zijn aan leverancier). Wel wordt getest op het begrip *Overeengekomen gebruik* welke ruimer is dan sec datgene wat in een programma van eisen staat (o.a. vanwege de in artikel 3 verwoorde zorgplicht);
- De resultaten van de Acceptatieprocedure worden schriftelijk vastgelegd in een testverslag. Dit verslag zal door partijen worden ondertekend. De gedachte is dat discussie achteraf over de uitkomsten van de acceptatietest op deze wijze tot een minimum wordt beperkt;
- Leverancier dient een planning af te geven voor het herstel van geconstateerde Gebreken. Die planning dient conform artikel 7.3 te passen binnen de algehele planning van het project;
- Na het herstel van de Gebreken legt de leverancier de ICT Prestatie opnieuw ter Acceptatie voor. Er volgt dan wederom een acceptatieprocedure conform de hiervoor beschreven uitgangspunten.

Artikel 7.3 is hiervoor al kort aangestipt. Het artikel bepaalt dat herstel van tijdens het testen geconstateerde Gebreken niet mag leiden tot vertraging. Het is dus aan de leverancier – mede gelet op zijn rol als penvoerder van het aanbod (artikel 3), het implementatieplan (artikel 5) en/of het testprotocol (artikel 7.1) – om op voorhand een realistische planning te hanteren met voldoende ruimte voor herstel van eventueel geconstateerde Gebreken.

In **artikel 7.4** staan de verschillende scenario's bij het niet slagen van de acceptatieprocedure vermeld:

1 ontbinding van de Overeenkomst; of
2 het alsnog kosteloos laten herstellen van de Gebreken; of
3 onder een nadere voorwaarde accepteren waarbij geldt dat indien niet aan de voorwaarde wordt voldaan alsnog direct kan worden ontbonden.

Deze drie smaken geven de gemeenten veel flexibiliteit in hoe om te gaan met eventuele gebreken:

1 indien kernaspecten van de ICT Prestatie niet goed zijn dan ligt ontbinding voor de hand;
2 bij kleine gebreken ligt kosteloos herstel voor de hand; en
3 bij het niet tijdig opleveren van onderdelen van de Prestatie die voor de gemeente pas in de toekomst relevant worden, ligt voorwaardelijke acceptatie voor de hand (namelijk acceptatie onder de voorwaarde dat de ICT Prestatie wel correct is geïmplementeerd op de datum dat de nu ontbrekende onderdelen voor de gemeente relevant worden).

In de GIBIT is er bewust voor gekozen na twee testrondes direct te kunnen ontbinden, zonder nadere ingebrekestelling. De gedachte is dat twee kansen om de overeengekomen prestatie te leveren in beginsel voldoende moet zijn. Bovendien wordt hiermee het preventief en zorgvuldig testen gestimuleerd.

Artikel 7.5 geeft partijen de ruimte om eventueel overeen te komen dat bepaalde gebreken buiten de staande planning worden hersteld.

Artikel 7.6 bepaalt uitdrukkelijk dat Gebreken die niet in de weg staan aan productieve ingebruikname, geen grond kunnen vormen voor niet-Acceptatie. De gedachte van de bepaling is dat een project niet op een formaliteit zou moeten worden afgekeurd, maar alleen op gebreken die daadwerkelijk relevant/wezenlijk zijn voor de gemeente. Dat laat overigens onverlet dat ook die minder relevante gebreken alsnog moeten worden hersteld. De levering van die betreffende functionaliteit is immers wel overeengekomen.

Artikel 7.7 bepaalt dat indien er deelleveringen hebben plaatsgevonden, dat dan na de laatste deellevering er ook nog een integrale Acceptatieprocedure plaatsvindt. Hiermee wordt uitdrukkelijk erkend dat bij ICT Prestaties de delen correct kunnen functioneren (voor zover te beoordelen als losstaand onderdeel), doch de som der delen niet, terwijl het de gemeente uiteraard om de som der delen (de totale ICT Prestatie) te doen is.

Artikel 7.8 geeft ten slotte een vermoeden van acceptatie aan indien de ICT Prestatie voor productieve doeleinden in gebruik is genomen, terwijl er geen acceptatieprocedure is afgesproken noch heeft plaatsgevonden. Deze dubbele voorwaarde is met name opgenomen vanwege noodgedwongen ingebruikname bij vertraging van het project. Het is denkbaar dat een gemeente bij vertraagde levering de ICT Prestatie noodgedwongen wel in gebruik moet nemen (bijv. omdat er anders geen ICT in huis is om een nieuwe wet te ondersteunen), maar dat wil daarmee niet zeggen dat de gemeente de ICT Prestatie (dus) ook geaccepteerd heeft. Als de gemeente echter zelf op voorhand bewust afziet van het houden van een Acceptatieprocedure en de ICT Prestatie vervolgens voor productieve doeleinden in gebruik neemt, dan aanvaardt ze daarmee impliciet dat de ICT Prestatie bij levering mogelijk nog Gebreken bevat, die vervolgens in het kader van Onderhoud (artikel 8) geadresseerd zullen (kunnen/moeten) worden.

Artikel 8. Onderhoud en ondersteuning

Uitgangspunt van de GIBIT is dat na de acceptatie de onderhoudsfase volgt. De GIBIT biedt een (abstract) kader voor de onderhoudsfase. Dit kader wordt in de praktijk veelal nader uitgewerkt in de overeenkomst of een afzonderlijke onderhoudsovereenkomst/SLA.

Vanwege het belang van blijvend goed functionerende ICT-systemen is er bewust voor gekozen om standaard te bepalen dat de leverancier Onderhoud verricht (**artikel 8.1**) en dat dit Onderhoud standaard alle in **artikel 8.3** genoemde vormen van onderhoud omvat. Uiteraard is het ook mogelijk dat in de overeenkomst juist wordt bepaald dat leverancier geen onderhoud verricht, of slechts een deel van de in artikel 8.3 genoemde vormen van onderhoud.

In **artikel 8.2** wordt het 'vangnet' karakter van de GIBIT wederom benadrukt. De bepalingen in de GIBIT gelden als basis, maar in de Overeenkomst of SLA kan hiervan worden afgeweken. De GIBIT bevatten weinig concrete normen ter zake van Onderhoud, behoudens enkele abstracte eisen (die hierna worden toegelicht). De concrete door de Leverancier na te leven normen (Service Levels) zullen dan ook in de Overeenkomst of SLA moeten worden opgenomen. Bovendien zullen allerlei praktische aspecten rondom het verlenen van Onderhoud nader moeten worden ingevuld (zoals hoe en waar een Gebrek gemeld moet worden). In veel gevallen is een dergelijke overeenkomst of SLA dan ook noodzakelijk.

In **artikel 8.4** is het uitgangspunt benoemd dat onderhoud zo min mogelijk verstorend moet zijn voor de bedrijfsprocessen van de gemeente. Er is bewust gekozen niets te bepalen over de precieze tijden waarop onderhoud wel/niet mag plaatsvinden, aangezien dat te zeer afhankelijk is van de precieze aard van de ICT Prestatie en de processen waarin deze wordt gebruikt.

Artikel 8.5 bepaalt dat de leverancier in ieder geval bereikbaar moet zijn op werkdagen tussen 08.00 en 18.00 uur. Er is bewust gekozen voor de term bereikbaar, zonder te specificeren welk kanaal of communicatiemiddel hierbij gebruikt moet worden. Dit laat leveranciers voldoende ruimte om dit zelf in te richten (telefoon, e-mail, chat, etc.).

Artikel 8.6 hangt samen met het hiervoor bij artikel 8.2 beschreven 'vangnet' karakter van de GIBIT. Het bepaalt dat leverancier bereid moet zijn een nadere SLA te sluiten. Een specifieke eis aan die SLA is dat er Service Levels in kunnen worden opgenomen en dat aan het niet halen van Service Levels maatregelen zijn verbonden. Welke maatregelen dat zijn, zal van geval tot geval nader moeten worden ingevuld. Het is voor de gemeente van belang dat de maatregel voldoende prikkel voor de leverancier geeft tot nakoming en bovendien iets oplevert waar de gemeente ook iets aan heeft.

In **artikel 8.7** is bepaald dat ontbinding van de overeenkomst(en) in ieder geval mogelijk is bij het herhaald niet halen van de service levels. Deze bepaling is opgenomen om uit de discussie te blijven of het niet halen van een service level altijd kwalificeert als tekortkoming en/of de discussie of

dergelijke omissies altijd de ontbinding van de overeenkomst rechtvaardigen. Bovendien is bepaald dat bedongen maatregelen de overige rechten van gemeenten onverlet laten. Dit om te voorkomen dat een in de SLA bedongen sanctie op grond van de wet zou gelden als gefixeerde schadevergoeding (artikel 6:92 lid 2 BW).

In **artikel 8.8** is bepaald dat indien Leverancier aantoont dat een Gebrek niet aan hem toerekenbaar is, hij alleen na afzonderlijke opdracht daartoe gehouden is tot herstel van het Gebrek. Te denken valt hierbij aan de situatie dat een medewerker van de gemeente in strijd met instructies van de leverancier belangrijke instellingen in de ICT Prestatie heeft gewijzigd, of dat door toedoen van een niet aan Leverancier toerekenbare virusuitbraak er allerlei herstelwerkzaamheden moeten worden verricht.

In **artikel 8.9** zijn enkele eisen opgenomen ten aanzien van het preventief en innovatief onderhoud. Het is voor gemeenten van groot belang dat blijvend wordt voldaan aan wet- en regelgeving, dat de interoperabiliteit gewaarborgd blijft en dat zij er niet in functionaliteit op achteruit gaat. Voor leveranciers is dit een zware eis, echter voor gemeenten een belangrijke. Vrijwel alle gemeentelijke producten, diensten, processen en informatieketens zijn immers op de een of andere manier gerelateerd aan het voldoen aan wet- en regelgeving. Door verdergaande digitalisering heeft dat effect op de kwaliteitseisen aan ICT-producten en diensten. De GIBIT gaat er derhalve vanuit dat de leverancier, als gespecialiseerde aanbieder van bepaalde programmatuur om bepaalde wetgeving te ondersteunen, veel beter dan de gemeente in staat is (zou moeten zijn) om wijzigingen in wetgeving tijdig te vertalen naar de benodigde (technische) aanpassingen in de ICT Prestatie. Let op: het ondersteunen van volstrekt nieuwe wetgeving valt veelal niet onder het ‘Overeengekomen gebruik’ (en daarmee het Onderhoud) en valt dus niet binnen de verplichting van dit artikel.

Artikel 8.10 geeft het kader voor de installatie van updates en upgrades. Uitgangspunt is dat de gemeente in beginsel zelf de installatie van updates en upgrades verzorgt. In artikel 8.10 is niettemin bepaald dat leverancier dit op verzoek (en tegen vergoeding) kan doen. In dat geval zijn ook de bepalingen omtrent implementatie en acceptatie van toepassing. In **artikel 8.11**

is getracht een genuanceerde regeling te treffen voor het weigeren van de installatie van nieuwe updates/upgrades. Enerzijds heeft de gemeente het recht die installatie te weigeren, anderzijds worden de verplichtingen van de leverancier in het kader van Onderhoud wat gerelativeerd indien de gemeente hiertoe besluit. Het artikel speelt niet in het geval van Hosting (zie de vooruitverwijzing naar artikel 31.4).

In **artikel 8.12** is opgenomen dat de leverancier in beginsel standaard rapporteert over de nakoming van de Service Levels. **Artikel 8.13** bepaalt vervolgens dat de gemeente na ontvangst van de rapportage zal beoordelen in hoeverre de leverancier de gemaakte afspraken naleeft. Eventueel kan op grond van artikel 21 hierbij een derde partij (auditor) worden ingeschakeld.

Artikel 8.14 vormt het sluitstuk van het vangnetkarakter van de GIBIT inzake onderhoud. Het bepaalt namelijk dat indien er initieel geen of slechts deels Onderhoud is overeengekomen, dat leverancier dan bereid moet zijn om op verzoek later alsnog Onderhoud te gaan verrichten of de bestaande overeenkomst inzake Onderhoud uit te breiden. Uiteraard geschiedt dit alles tegen een nader overeen te komen vergoeding. Het belang voor de gemeente is er met name in gelegen dat zij zeker weet dat ze altijd alsnog tot het afnemen van onderhoud kan overgaan.

Artikel 9. Vergoeding, facturatie en betaling

In **artikel 9.2** is een iets andere benadering gekozen dan de ARBIT doet. Waar de ARBIT uitgaat van volledige voorfinanciering door de leverancier, kiest de GIBIT ervoor slechts een deel van de betalingen achter te houden tot na acceptatie. Dit in de gedachte dat het onredelijk is het gehele financiële risico van het project bij de leverancier te leggen, doch tegelijkertijd voldoende (financiële) prikkel voor de leverancier over te houden om tot correcte implementatie te komen. In dat kader is voor de meeste vergoedingen bepaald dat 30% wordt achtergehouden tot Acceptatie. De GIBIT erkent voorts dat bij Derdenprogrammatuur de leverancier veelal zelf direct moet betalen. Vandaar dat bij Derdenprogrammatuur geen sprake is van het achterhouden van een deel van de vergoeding maar betaling na levering geschiedt. Overigens, dit geldt enkel voor Derdenprogrammatuur welke conform artikel 19 vooraf aan de gemeente kenbaar is gemaakt.

Artikel 9.3 geeft de mogelijkheid in de Overeenkomst nadere eisen te stellen ten aanzien van de factuur.

Artikel 9.4 stelt als standaard betaaltermijn 30 dagen.

Artikel 9.5 bepaalt dat er standaard elektronisch moet worden gefactureerd conform de daarvoor geldende standaard.

In **artikel 9.6** en **9.7** zijn regelingen omtrent prijsverhogingen doorgevoerd. Hoofdregel is dat alleen de prijsstijging uit de dienstenprijsindex gevolgd mogen worden (artikel 9.6). Opnieuw wordt hier de nuance gezocht ten aanzien van Derdenprogrammatuur: hier mogen niet voorzienbare prijsstijgingen aan gemeenten worden doorbelast mits deze aantoonbaar worden gemaakt.

Artikel 9.8 bepaalt dat vergoedingen die gerelateerd zijn aan wijzigingen onderhevige getallen die zijn gerelateerd aan Opdrachtgever, slechts éénmaal per jaar worden bijgesteld en wel op 1 januari. De gedachte is dat hierdoor prijsschommelingen gedurende de looptijd worden beperkt.

Artikel 9.9 bepaalt dat hetgeen in dit artikel omtrent Derdenprogrammatuur is bepaald alleen geldt voor zover leverancier heeft voldaan aan hetgeen in artikel 19.1 is bepaald. Artikel 19.1 bepaalt dat leverancier de relevante Derdenprogrammatuur uitdrukkelijk in zijn aanbod moet specificeren. Met andere woorden: indien leverancier verzaakt de relevante Derdenprogrammatuur te specificeren, dan geniet hij ook niet de voordelen van genuanceerde betalingsregeling zoals verwoord in dit artikel (en wordt dus ook bij die programmatuur 70% bij ingebruikname en 30% bij integrale acceptatie betaald).

Artikel 10. Garanties

In dit artikel worden in het **eerste lid** diverse garanties vermeld. De meeste garanties spreken voor zich en zien er met name op dat de leverancier er voor in staat dat hij zal levert wat is overeengekomen.

De garantie onder iii hangt samen met artikel 8.14 inzake Onderhoud. Het is voor gemeenten van belang om desnoods op een later moment alsnog Onderhoud af te kunnen nemen. Het is daarvoor noodzakelijk dat de geleverde

ICT Prestatie daadwerkelijk nog onderhouden wordt. In dit artikel geeft de leverancier de garantie dat dit in ieder geval twee jaar na Acceptatie nog het geval is.

Artikel 10.2 vermeldt een belangrijk gevolg van de garanties, namelijk dat indien de gemeente een garantie inroept, dat het dan aan de leverancier is om aan te tonen dat het beroep onterecht is. Het artikel bevat in zoverre een bewijslastverdeling.

Artikel 11. Documentatie

Het **eerste lid** van dit artikel bepaalt dat leverancier documentatie dient te leveren. Ook stelt het artikel enkele eisen aan de documentatie. Documentatie wordt hier in brede zin gebruikt: het artikel ziet zowel op het gebruik van de geleverde ICT Prestatie (sub i, sub iii), op het documenteren van de door Leverancier gemaakte instellingen (sub ii), op het kunnen uitvoeren van de acceptatietesten (sub iv) en op het beheren van de ICT Prestatie (sub v). Daarbij kan voor het nakomen van sub v de GEMMA Softwarecatalogus (www.softwarecatalogus.nl) deels worden gebruikt.

Om leveranciers voldoende flexibiliteit te geven, is bepaald dat alleen de documentatie gericht op eindgebruikers in het Nederlands gesteld dient te zijn. Overige documentatie mag ook in het Engels zijn opgesteld.

Artikel 11.2 en **11.3** zien op het tijdig aanleveren van de documentatie. **Lid 2** bepaalt dat de documentatie in ieder geval voorafgaand aan de Acceptatieprocedure en bij de levering van Updates en Upgrades moet worden geleverd. Het **derde lid** bepaalt in algemene zin dat leverancier de documentatie moet updaten zodra blijkt dat deze niet langer juist is.

Artikel 12. Productmanagement

Het is voor gemeenten van belang tijdig op de hoogte te zijn en blijven omtrent de ontwikkelingen van de ICT Prestatie. Vandaar dat in dit artikel is opgenomen dat de gemeente tijdig over de roadmap wordt geïnformeerd (**artikel 12.1**) en toegang krijgt tot organen/platformen waar ervaringen met en informatie over de ICT Prestatie wordt uitgewisseld (**artikel 12.2**). Beide aspecten staan los van eventueel overeengekomen onderhoud.

Voorts zijn in dit artikel in het **derde lid** bepalingen opgenomen over uitbreidingen op bestaande programmatuur die op maat en op kosten van een gemeente zijn ontwikkeld. Het artikel bepaalt dat de leverancier (1) andere gebruikers van de programmatuur moet informeren over de uitbreiding, waaronder of de uitbreiding wordt opgenomen in toekomstige versies en (2) de uitbreiding aan andere gebruikers kosteloos ter beschikking moet stellen. De gedachte is dat meer gemeenten van deze uitbreidingen profijt hebben. Het artikel bepaalt verder dat het gebruik van de aldus ter beschikking gestelde uitbreiding voor eigen risico van de gemeente is, tenzij de uitbreiding op kosten van de gemeente zelf is ontwikkeld of als onderdeel van een Update of Upgrade in het kader van Onderhoud ter beschikking wordt gesteld. De gedachte hiervan is dat het zowel voor de gemeente als de leverancier het meest aantrekkelijk is om uitbreidingen onder te brengen in het standaard product en het standaard onderhoudsprogramma.

Artikel 13. Aansprakelijkheid

Het artikel over aansprakelijkheid is geïnspireerd op de ARBIT, maar kiest ook een eigen koers. Die eigen koers blijkt met name uit het **tweede** en het **vierde lid** van het artikel.

In het **tweede lid** staan de schadesoorten vermeld die bij aansprakelijkheid van de leverancier voor vergoeding in aanmerking komen. Deze lijst is bedoeld om discussies over schade (direct/indirect, causaliteit, etc.) te verminderen en juist vooraf voor beide partijen helder te hebben welke schadesoorten relevant (kunnen) zijn. Bij de concrete toepassing van het artikel kan er altijd als nog discussie zijn of een bepaalde schadepost onder een bepaald artikel valt en of de betreffende concrete schade niet in een te ver verwijderd verband van de schadeoorzaak staat. Dat een bepaalde schadesoort (in abstracto) voor vergoeding in aanmerking komt, is hiermee echter evident.

In het **vierde lid** is een genuanceerdere regeling getroffen in vergelijking met de ARBIT. In de kern staat hier dat wanneer de gemeente een boete opgelegd krijgt van een toezichthouder vanwege een situatie die rechtstreeks toe te rekenen is aan een toerekenbare tekortkoming of een toerekenbaar gedragen of nalaten van de leverancier (lees: een onrechtmatige daad), dat de leverancier de gemeente voor die boete moet vrijwaren (althans voor dat

deel dat aan de leverancier is toe te rekenen). Dit is een situatie die zich in de praktijk niet zo snel zal voordoen (gelet op o.m. het *ultimum remedium* karakter van boetes). De vraag is bovendien of er geen sprake is van opzet of grove schuld van de leverancier indien de gemeente een boete krijgt voor een situatie die toerekenbaar is aan de leverancier. Juist om die discussie te voorkomen is niettemin opgeschreven dat de leverancier de gemeente voor dergelijke boetes vrijwaart.

Voor de goede orde merken wij op dat naast de bepalingen in de GIBIT het Burgerlijk Wetboek (en andere wetgeving) onverkort van toepassing is, tenzij daar in de GIBIT uitdrukkelijk van is afgeweken. Dat uitgangspunt geldt voor de hele GIBIT en (dus) ook voor het thema aansprakelijkheid. Dit houdt o.m. in dat de regels uit boek 6 titel 1 afdeling 10 (over schadevergoeding) van toepassing zijn, waaronder begrepen de daarin opgenomen regels omtrent schadebegroting, causaliteit, eigen schuld, etc. Ook in de situaties van **artikel 13.3, 13.4** en **13.5** is de aansprakelijkheid van leverancier dus niet onbeperkt (maar beperkt door de kaders van het BW).

Artikel 14. Verzekering

In **artikel 14** is bepaald dat leverancier voldoende zekerheid moet bieden voor verhaal, hetzij via een verzekering, hetzij anderszins. Er is bewust voor gekozen een verzekering niet dwingend voor te schrijven. Er zijn immers legio manieren denkbaar waarop het risico voor gemeenten dat de leverancier in voorkomend geval geen verhaal biedt, afgedekt kan worden (moedergarantie, bankgarantie, derdenrekening, etc.).

In het **tweede lid** is een minimumdekking opgenomen. Deze dekking correspondeert met de maximale aansprakelijkheid zoals dit in het vorige artikel is bepaald.

Artikel 15. Geheimhouding

Artikel 15 regelt een wederkerige geheimhoudingsverplichting. In het **eerste lid** is bepaald dat beide partijen alle informatie waarvan zij het vertrouwelijke karakter (behoren te) kennen geheim zullen houden. Partijen worden uit de geheimhouding ontheven voor zover dit noodzakelijk is op grond van een wettelijk voorschrift, onderzoek van een toezichthouder of gerechtelijke procedures.

Verder is uitdrukkelijk in **lid 1** bepaald dat gemeenten de inhoud van de overeenkomst met andere gemeenten mogen delen. De gedachte is dat hierdoor meer prijstransparantie op de markt zal gaan ontstaan.

In het **tweede lid** is opgenomen dat beide partijen de geheimhouding ook zullen opleggen aan door hen ingeschakeld personeel en hulppersonen.

Het **derde lid** bepaalt dat vertrouwelijke gegevens op verzoek moeten worden teruggeven.

Het **vierde lid** ten slotte stelt voor alle partijen een boete op het schenden van de geheimhoudingsplicht. Er is een boete opgenomen omdat het begroten van de schade bij schending van de geheimhouding in de praktijk veelal niet eenvoudig is. Zodoende zou iedere prikkel tot het geheim houden van vertrouwelijke informatie zonder boetebeding kunnen ontbreken (bij niet te begroten schade volgt immers toch geen schadeclaim). De boete is gemaximeerd op € 50.000,–.

Artikel 16. Overmacht

Het **eerste lid** van dit artikel herhaalt in feite wat er in de wet omtrent overmacht staat.

Het **tweede lid** expliceert dat bepaalde omstandigheden in ieder geval niet als overmacht worden gekwalificeerd. De in dit lid genoemde omstandigheden komen dus voor risico van de leverancier.

Ten aanzien van uitval van nuts- en telecomvoorzieningen is een genuanceerde regeling getroffen. In beginsel kwalificeert uitval van dergelijke diensten als overmacht. De GIBIT erkent daarmee dat leveranciers dergelijke diensten zelf ook inkopen en daarbij veelal niet in de positie zijn om een bepaald niveau van dienstverlening af te dwingen. Van overmacht is echter geen sprake indien de storing door leverancier zelf is veroorzaakt of wanneer is overeengekomen dat leverancier de nuts- of telecomvoorzieningen beschikbaar diende te houden. Ter illustratie van dit laatste: voor een cloud-/ASP-dienst betekent dit veelal dat het de leverancier wel kan worden aangerekend als zijn eigen verbinding naar het publieke internet toe uitvalt (dit is dan geen

overmacht), maar niet indien er op het publieke internet of bij de provider van de gemeente storingen zijn die maken dat er geen gebruik kan worden gemaakt van de cloud-/ASP-dienst.

Artikel 17. Intellectuele eigendom

Tijdens de totstandkoming van de GIBIT is ten aanzien van intellectuele eigendom onderscheid gemaakt tussen drie situaties:

1. de leverancier levert een standaardproduct;
2. de leverancier ontwikkelt op verzoek en op kosten van gemeente een aanvulling op een standaardproduct;
3. de leverancier ontwikkelt op verzoek van de gemeente een autonoom functionerend programma.

In de eerste situatie ligt het voor de hand dat de gemeente louter een gebruiksrecht verkrijgt en geen andere aanspraak op de intellectuele eigendomsrechten. Dit komt in **artikel 17.3** naar voren. De duur van de gebruiksrechten verschilt naar gelang de aard van de vergoeding: bij periodieke vergoedingen is de duur van het gebruiksrecht gelijk aan de looptijd van de overeenkomst, bij overige vergoedingen is sprake van een eeuwigdurend gebruiksrecht. De koppeling aan de duur van de overeenkomst (en niet: aan de betaalfrequentie) bij periodieke vergoedingen is bewust; voorkomen moet worden dat het niet tijdig betalen automatisch tot verval van het gebruiksrecht leidt.

De tweede hiervoor beschreven situatie kan zich onder allerlei omstandigheden voordoen. Zo kan de aanvulling op het product zeer specifiek op de omstandigheden bij een bepaalde gemeente toegeschreven zijn (in welk geval overdracht van IE-rechten voor de hand zou kan liggen), maar is evengoed denkbaar dat de aanvulling op het product in feite zo generiek van aard is dat ook andere gemeenten daarvan zouden kunnen profiteren (in welk geval een terugverdienregeling en/of een doorslaggevende stem bij de verdere productontwikkeling wellicht logischer is). Juist omdat het een aanvulling op een standaardproduct betreft, en de broncode van de aanvulling dus sterk verband zal hebben met de broncode van het standaardproduct, ligt terbeschikkingstelling van broncodes in veel situaties niet voor de hand (bedrijfsgeheim). Overdracht van IE-rechten zal in veel gevallen om soortgelijke redenen

lastig liggen. Het voorgaande laat onverlet dat bij dergelijke situaties in feite sprake is van door de belastingbetaler gefinancierde productontwikkeling. Vandaar dat is bepaald dat die aanvullingen kosteloos aan andere gebruikers van de betreffende programmatuur ter beschikking moeten worden gesteld. Zie daarvoor de nadere toelichting bij artikel 12. Het staat partijen vrij in voorkomend geval in de overeenkomst te bepalen dat **artikel 17.4** niet van toepassing is, in welk geval het bepaalde in artikel 12.3 ook niet geldt.

In de derde situatie wordt specifiek voor de gemeente een autonoom programma ontwikkeld. Het ligt dan voor de hand dat de gemeente ook de beschikking krijgt over de rechten en de broncodes van dat zelfstandige programma. Dat is dan ook in **artikel 17.5** bepaald. In **artikel 17.6** wordt direct de nuance hierbij gezocht: de gemeente verklaart zich hierin bij voorbaat bereid om in gesprek te gaan om de rechten terug over te dragen. Partijen zullen in overleg moeten treden onder welke voorwaarden die overdracht plaatsvindt.

In **lid 6** en **7** is geborgd dat de gemeente gebruik kan blijven maken van de voor haar relevante functionaliteit bij claims van derden dat de gebruikte ICT Prestatie inbreuk maakt op hun rechten. In **lid 8** is bepaald dat bij een aansprakelijkstelling door de betreffende derde, de gemeente de overeenkomst ook moet kunnen ontbinden. Deze laatste bepaling is met name bedoeld om de schade voor de gemeente te kunnen beperken. De gemeente moet een aansprakelijkstelling immers in de administratie opnemen en heeft zodoende een (boekhoudkundige) prikkel om de (vermeende) inbreuk zo snel mogelijk te (kunnen) staken. In de praktijk zal vermoedelijk weinig een beroep worden gedaan op **lid 8** en zal met name de (meer praktisch gerichte) benadering van **lid 6** en **7** relevant zijn.

Artikel 18. Toegang tot data

Het is voor de gemeenten van groot belang dat zij toegang blijven houden tot de met de ICT Prestatie verwerkte data (hun eigen data). Gemeenten wensen de betreffende gegevens ook buiten de door de leverancier geleverde prestatie en/of voor andere doeleinden en in andere processen en systemen te kunnen gebruiken, zoals business intelligence toepassingen of big data analyses voor managementinformatie en/of in bedrijfssystemen die deel uitmaken van de proces- en informatieketen.

Dit artikel bepaalt in **lid 1** dat leverancier opdrachtgever in staat moet stellen die toegang te allen tijde te verkrijgen. De wijze waarop leverancier daar invulling aan geeft, is open gelaten. In **lid 2** zijn slechts enkele voorbeelden opgenomen. In de praktijk kan leverancier ook op andere wijzen aan de verplichting uit **lid 1** voldoen.

Het laatste lid bepaalt dat het gebruik van de gegevens door de gemeente voor eigen rekening en risico is. Wel moet de leverancier de gemeente waarschuwen indien het verlenen van toegang ertoe leidt dat bepaalde beveiligingen worden omzeild (**lid 3**). De gemeente kan zo een geïnformeerde keuze maken over het gebruik van de data.

Artikel 19. Derdenprogrammatuur

In de GIBIT is een afzonderlijke regeling opgenomen voor Derdenprogrammatuur. Dit begrip is gedefinieerd in artikel 1.7. Er wordt gedoeld op programmatuur van externe leveranciers die niet gelieerd zijn aan de leverancier en op welke ontwikkeling leverancier verder ook geen invloed heeft. Er kan worden gedacht aan programmatuur van partijen als Microsoft, Oracle, Adobe, Google, IBM, HP, SAP, etc.

De regeling van **artikel 19** is opgenomen omdat erkend wordt dat leveranciers veelal geen invloed hebben op de kwaliteit/functionaliteit van deze Derdenprogrammatuur, noch op de voorwaarden waaronder deze Derdenprogrammatuur op de markt wordt gebracht.

In **lid 1** is bepaald dat leverancier moet specificeren of sprake is van Derdenprogrammatuur en zo ja, welke licentievoorwaarden gelden. De gedachte is dat de gemeente zo een geïnformeerd besluit kan nemen over het al dan niet accepteren van die voorwaarden. Die voorwaarden prevaleren namelijk op hetgeen elders in de overeenkomst is bepaald (**lid 6**).

In **lid 2** is bepaald dat de leverancier moet aangeven of de betreffende Derdenprogrammatuur ook elders te verkrijgen is. De ervaring leert dat veel Derdenprogrammatuur ook bij andere leveranciers te krijgen is, of wellicht al eerder door de gemeente is aangeschaft. De specificatie maak dat de gemeente kan besluiten de Derdenprogrammatuur niet of bij een andere leverancier aan te schaffen.

Op grond van het **derde lid** moet de leverancier ook de eventuele afhankelijkheid van Derdenprogrammatuur in het aanbod specificeren. De ervaring leert dat bij discussies over bijvoorbeeld performance (te) snel wordt gewezen op programmatuur van derden. Door vooraf te worden geïnformeerd over die afhankelijkheid, kan de gemeente ook op dit punt een geïnformeerde keuze maken. Bovendien wordt zo oneigenlijk gebruik van dit argument voorkomen.

In het **vierde lid** is bepaald dat de leverancier tijdig Updates en Upgrades moet uitbrengen teneinde de compatibiliteit met Derdenprogrammatuur te blijven borgen. Hierbij kan bijvoorbeeld gedacht worden aan de situatie dat de ICT Prestatie niet meer functioneert na een update van de Derdenprogrammatuur, of de situatie dat de Derdenprogrammatuur zelf (om wat voor reden dan ook) niet langer functioneert.

Het bepaalde in **lid 5** en **6** vormt het sluitstuk van de afhankelijkheid van Derdenprogrammatuur. Vrij vertaald staat hier dat een leverancier vrijuit gaat indien een gebrek in de door hemzelfde geleverde prestatie (veelal: software) wordt veroorzaakt door een fout in de Derdenprogrammatuur, tenzij hij die laatstgenoemde fout had behoren te kennen en er om heen had kunnen werken. Eventueel overeengekomen service levels e.d. gelden dus in dat geval ook niet. Wel moet de leverancier er dan alsnog zo snel mogelijk alles aan doen om het probleem zo snel mogelijk op te lossen (**lid 6**).

De leverancier kan niet van deze (royale) uitzondering op de onderhoudsverplichtingen profiteren indien hij niet de hiervoor gespecificeerde informatie heeft gegeven (**lid 7**). De leverancier schiet in dat geval in beginsel bovendien tekort in de nakoming van de betreffende verplichtingen. Dat zou in principe een ontbinding of mogelijk vernietiging (wegens dwaling) van de overeenkomst kunnen rechtvaardigen. Wel moet dan steeds van geval tot geval bezien worden hoe zwaar dat achterhouden van de betreffende informatie door de leverancier in concreto heeft meegewogen.

Artikel 20. Opschorting, opzegging en ontbinding

In dit artikel zijn enkele bepalingen opgenomen in het belang van de gemeente. Zo is een beroep van de leverancier op opschorting aan banden gelegd (**artikel 20.1**). De gemeente is immers veelal in grote mate afhankelijk van

de leverancier, terwijl het normale wettelijke systeem de leverancier vrij laagdrempelig toestaat zich op opschorting te beroepen.

In **artikel 20.2** is bepaald dat overeenkomsten voor bepaalde tijd in beginsel niet tussentijds kunnen worden opgezegd en dat overeenkomsten voor onbepaalde tijd in beginsel altijd kunnen worden opgezegd met inachtneming van de vermelde opzegtermijnen. De bepaling houdt verband met het bepaalde in artikel 7:408 BW.

In **artikel 20.3** is bepaald dat samenhangende overeenkomsten – ondanks die samenhang – selectief kunnen worden opgezegd tegen het einde van de actuele looptijd. Hierbij kan bijvoorbeeld gedacht worden aan het opzeggen van de onderhoudsovereenkomst, terwijl de hostingovereenkomst doorloopt. De bepaling kan overigens ook worden gelezen als selectief verlengen.

In de **artikelen 20.4** en **20.5** is bepaald dat de gemeente de overeenkomst(en) moet kunnen opzeggen bij fusie, uitbesteding en de verplichte overstap naar landelijke voorzieningen. De gedachte bij al deze bepalingen is dat de gemeente zonder een dergelijke bevoegdheid in voorkomend geval niet van bestaande overeenkomsten af zou kunnen en aldus zou moeten blijven betalen voor dienstverlening die voor haar van geen waarde meer is.

In **artikel 20.6** is bepaald dat de leverancier gerechtigd is om – kort samengevat – de daardoor geleden schade bij de gemeente in rekening te brengen. Bij die schadeberekening moet rekening worden gehouden met mogelijke hernieuwde inzet van productiemiddelen door leverancier. Dit om te voorkomen dat leverancier voor hetzelfde productiemiddel zowel een schadevergoeding van de gemeente ontvangt, als (bij een andere klant) daarmee opnieuw winst realiseert.

In de **artikelen 20.7-20.11** zijn de verschillende ontbindingsgronden nader uitgewerkt. Naast de wettelijke gronden voor ontbinding, zijn hier ook de gebruikelijke gronden (zoals faillissement leverancier) aan toegevoegd. Verder is voorzien in ontbinding bij een vernietiging van een overeenkomst op grond van de Aanbestedingswet en bij langdurige overmacht.

Artikel 21. Controlerecht en medewerking audits bij Opdrachtgever

Dit artikel ziet op twee verschillende (en niet-gerelateerde) soorten controles/audits: enerzijds het door opdrachtgever controleren van leverancier (**lid 1-5**) en anderzijds het medewerking verlenen van leverancier aan audits die bij opdrachtgever worden uitgevoerd (**lid 6**).

Opdrachtgever is gerechtigd om een onafhankelijke derde te laten controleren of leverancier de overeengekomen verplichtingen nakomt (**lid 1**). Ook mag de juistheid van de facturen worden onderzocht (**lid 1**).

Er is in het kader van de redelijkheid toegevoegd dat de controle moet zien op de nakoming van wezenlijke verplichtingen. Om diezelfde reden is ook toegevoegd dat een controle alleen gerechtvaardigd is indien er gerede twijfel is over de nakoming door de leverancier, of indien er een ander gerechtvaardigd belang voor de gemeente is.

De leverancier moet aan de controle alle redelijkerwijs te verwachten medewerking verlenen (**lid 3**). De kosten voor de controle zijn voor de gemeente, tenzij de deskundige relevante tekortkomingen van leverancier constateert (**lid 4**). Deze laatste regel maakt dat een gemeente terughoudend en prudent zal omspringen met het aantal uit te voeren controles.

De gemeente zelf kan ook onderworpen zijn aan audits. Het kan in dat kader relevant zijn om meer informatie te kunnen verschaffen over de gebruikte ICT-prestaties. Veelal zal de gemeente die informatie zonder medewerking van de leverancier kunnen verschaffen. Er zijn echter omstandigheden denkbaar waarbij medewerking van de leverancier noodzakelijk is. Voor die omstandigheden bepaalt **lid 6** dat de leverancier alle medewerking zal verlenen aan een dergelijke audit.

Artikel 22. Overstap naar ander systeem, afschaling voor archiefdoeleinden en overdracht

Artikel 22 vormt het sluitstuk op de ‘life cycle’ benadering van de GIBIT. Dit artikel beschrijft diverse situaties waarbij de gemeente de ICT Prestatie niet langer gebruikt en wat er (in voorbereiding daarop) in dat geval dient te gebeuren voor een soepele overstap.

In **artikel 22.1** is allereerst vastgelegd dat partijen op verzoek van de gemeente over zullen gaan tot het opstellen van een exit-plan. Het artikel ziet louter op het opstellen van het plan als zodanig. In het plan kunnen één of meer van de in de volgende artikelleden beschreven opties nader worden uitgewerkt.

De eerste optie die in dit kader wordt beschreven is dat van het exit-scenario (**artikel 22.2-22.5**). Dit scenario ziet op de overstap op een ander systeem, of de overdracht van het beheer van het bestaande systeem aan een ander. De leverancier wordt verplicht om daaraan mee te werken. Doel is een *vendor lock-in* situatie te voorkomen.

De tweede optie die wordt beschreven is het verkrijgen van nieuwe licenties voor beperkt gebruik (artikel **22.6-22.8**). De gedachte is dat de bestaande (ruime) licenties niet langer nodig zijn, maar de gemeente middels beperkte licenties (bijv. alleen inzagerechten, geen gebruik van de software) in ieder geval nog een basis kan borgen om bij bepaalde data te kunnen. In **artikel 22.8** is bepaald dat deze mogelijkheid niet beschikbaar is bij Hosting. De gedachte daarvan is dat het gebruik van beperktere licenties alleen zinvol is bij *on premise* software en niet bij gehoste software.

De derde optie die wordt geboden is dat de ICT Prestatie wordt overgedragen aan een gemeenschappelijke regeling of andere publieke entiteit **(artikel 22.9**). Dit artikel geldt in aanvulling op het bepaalde in artikel 20.4. Laatstgenoemde artikel biedt een grond om de overeenkomst op te zeggen, artikel 22.9 biedt een grond om de overeenkomst over te dragen. Aangezien bij overdracht allerlei werkzaamheden zullen moeten worden verricht is de bepaling in artikel 22 opgenomen. Dit maakt immers dat het exit-plan van artikel 22.1 van toepassing is op deze werkzaamheden.

Tenslotte wordt in algemene zin bepaald dat (kort gezegd) gedurende de uitvoering van de exit-werkzaamheden de overeenkomst van kracht blijft c.q. verlengd wordt (**artikel 22.10**). Dit om te voorkomen dat de gemeente in een situatie terecht komt waarbij ze tijdelijk geen enkel systeem heeft (geen oud systeem meer, maar ook nog geen nieuw systeem).

Artikel 23. Toepasselijk recht en geschillen

In **artikel 23** is bepaald dat de overeenkomst wordt beheerst door Nederlands Recht, dat het Weens Koopverdrag niet van toepassing is en dat geschillen zullen worden beslecht door de rechter in het arrondissement van de Opdrachtgever.

Er is bewust gekozen voor de overheidsrechter en niet voor arbitrage. Afwegingen hierbij zijn o.m. kosten en de openbaarheid van de zitting. Het is voor overheidsorganen van belang dat publiekelijk verantwoording wordt afgelegd over de besteding van belastinggeld. Het past in dat kader niet om geschillen standaard middels (in beginsel) geheime en veelal kostbare arbitrageprocedures af te doen.

Het is wel denkbaar dat in voorkomend geval (alsnog) voor arbitrage gekozen wordt. Partijen zullen daar dan – bij contractering of achteraf – overeenstemming over moeten zien te bereiken. Met name de specifieke deskundigheid van de arbiters kan in dat kader een relevante afweging zijn.

II. Privacy, beveiliging en archivering

In dit hoofdstuk zijn enkele specifieke artikelen opgenomen over privacy, beveiliging en archivering. Het hoofdstuk is van toepassing zodra er gegevens met de ICT Prestatie worden verwerkt. Dat zal heel vaak het geval zijn, maar zeker niet altijd (bijv. niet bij verkoop hardware).

Artikel 24. Bewerkersrelatie

Artikel 24 ziet op de verhouding tussen partijen en de in dat kader al dan niet aanvullend te maken afspraken. Leverancier neemt de rol van bewerker in. De GIBIT heeft in dit kader te gelden als (basis)bewerkersovereenkomst (**artikel 24.2**). Daar waar de afspraken uit de GIBIT niet volstaan, kan een aanvullende of afwijkende bewerkersovereenkomst worden gesloten (**artikel 24.3**).

In **artikel 24.4** wordt uitdrukkelijk de ruimte geboden om sub-bewerkers in te schakelen. Een verbod op sub-bewerkers zou in de praktijk namelijk te zeer knellen. De GIBIT stelt wel allerlei randvoorwaarden aan de inschakeling van de betreffende sub-bewerkers.

Artikel 25. Verwerking persoonsgegevens

In **artikel 25** komen de meeste afspraken uit een bewerkersrelatie terug. Zo is bepaald dat leverancier de gegevens niet voor eigen doeleinden mag gebruiken (**lid 2**), dat hij de gegevens op passende wijze moet beveiligen (**lid 3**), dat een algemene beschrijving van de genomen beveiligingsmaatregelen wordt vastgelegd **(lid 4**), dat de gegevens met inachtneming van gedragscodes en wet- en regelgeving moeten worden verwerkt (**lid 5**), dat gegevens louter binnen de EER worden verwerkt (**lid 6**), dat de gegevens geheim moeten worden gehouden (**lid 7**), dat de gemeente de bewerker mag controleren (**lid 8**) en dat bij uitoefening van rechten door de betrokkene de leverancier in beginsel verwijst naar de gemeente (**lid 9**).

Gemeenten worden er uitdrukkelijk op gewezen dat zij – als verantwoordelijke – het beleid ten aanzien van de verwerking van persoonsgegevens dienen te bepalen. Dit betekent dus ook dat de gemeenten in principe het beveiligingsbeleid van de leverancier dienen te dicteren, althans op zijn minst te toetsen of het door de leverancier gehanteerde beleid aan minimaal dezelfde normen voldoet als het beleid van de gemeente.

Artikel 26. Informatiebeveiliging

Artikel 26 ziet specifiek op beveiliging. Het artikel heeft enerzijds het karakter van een garantie, in de zin dat leverancier er op grond van het eerste lid voor in moet staan dat de Opdrachtgever met de ICT Prestatie kan voldoen aan de Baseline Informatie Beveiliging van KING, althans een andere overeengekomen norm van informatiebeveiliging (**lid 1**).

Anderzijds bevat het artikel ook een verplichting in die zin dat als de ICT Prestatie door de leverancier beheerd of verricht wordt, dat de leverancier er dan voor moet zorgen dat de ICT Prestatie feitelijk aan die norm voldoet (**lid 2**).

Het **derde lid** bepaalt dat de leverancier er voor in staat dat ingeschakeld personeel zich aan de normen houdt.

In het **vierde lid** is uitdrukkelijk bepaald dat informatie over de getroffen beveiligingsmaatregelen vertrouwelijk is.

Artikel 27. Meldplicht beveiligingsincidenten

Artikel 27 geeft een uitwerking van de verplichtingen die voortvloeien uit de meldplicht datalekken en soortgelijke wetgeving (bijvoorbeeld de mogelijke meldplicht voor vitale infrastructuur die wellicht ook nog volgt).

Het artikel is als volgt opgebouwd:

- **Lid 1** bepaalt dat de leverancier de gemeente zal informeren over inbreuken en incidenten;
- In **lid 2** is opgenomen dat de melding in beginsel door de gemeente wordt gedaan;
- Op grond van **lid 3** moet de leverancier meewerken aan het zo nodig verschaffen van (aanvullende) informatie aan betrokkenen of toezichthouders;
- Het vierde lid bepaalt dat de leverancier de werkzaamheden op grond van dit artikel kosteloos verricht, tenzij leverancier aantoont dat de inbreuk niet aan hem toerekenbaar is (**lid 4**). De ratio hiervan is dat de leverancier moet voorzien in 'passende', maar niet in 'perfecte' beveiliging en dat (dus) niet iedere inbreuk het gevolg zal zijn van een tekortkoming van leverancier. Als van die tekortkoming wel sprake is, verricht leverancier de werkzaamheden dus (bij wijze van schadevergoeding) kosteloos, in andere gevallen worden deze op basis van nacalculatie verricht;
- Op grond van respectievelijk het **vijfde** en het **zesde lid** moet leverancier een logboek bijhouden van incidenten en daar inzage in verlenen;
- **Lid 7** bepaalt dat leverancier aansprakelijk is voor de gevolgen van incidenten en dat bij schending van het artikel geen nadere ingebrekestelling vereist is;
- Het **8e lid** ten slotte bepaalt dat de verplichtingen niet van toepassing zijn voor zover de door het incident getroffen gegevens niet van de gemeente afkomstig zijn of de gemeente daarvoor niet verantwoordelijk is. Dit hangt samen met het gegeven dat veel leveranciers gegevens van verschillende gemeenten tegelijkertijd verwerken en niet ieder incident betrekking zal hebben op al die gegevens.

Artikel 28. Archivering

Typerend voor de overheidsmarkt is de gebondenheid aan de Archiefwet. In dit artikel zijn daarom enkele randvoorwaarden opgenomen. Het **eerste lid** bepaalt dat de leverancier zorg moet dragen voor het aantoonbaar beheren en beschermen van de bewaarde gegevens overeenkomstig daartoe in de Gemeentelijke ICT-kwaliteitsnormen gestelde eisen. Het **tweede lid** bepaalt dat de leverancier gegevens overeenkomstig de in die normen gestelde termijnen moet bewaren. Het **derde lid** bepaalt dat de leverancier de archiefbescheiden moet kunnen migreren naar archiefsystemen van de gemeente, overeenkomstig de Gemeentelijke ICT-kwaliteitsnormen. Het artikel zal in de praktijk enige overlap (kunnen) vertonen met het in artikel 22.3 en 22.4 beschreven deel van het Exit-scenario. Het **vierde lid** is opgenomen omdat (met name bij Hosting) denkbaar is dat de leverancier de enige partij is die feitelijk over de archiefbescheiden beschikt. Het artikel stelt buiten alle twijfel dat leverancier die gegevens moet (terug)leveren aan de gemeente bij opschorting, opzegging of ontbinding van de overeenkomst. Het is de leverancier dus niet toegestaan die gegevens te 'gijzelen'. Ook hier geldt dat er enige overlap is met het in artikel 22.3 en 22.4 beschreven Exit-scenario.

III. Hosting

In dit hoofdstuk zijn enkele specifieke artikelen opgenomen voor het geval de ICT Prestatie (mede) Hosting omvat. Het begrip 'Hosting' is bewust abstract en vrij breed gedefinieerd (zie artikel 1.13). Het omvat niet alleen de dienstverlening die klassiek onder 'hosting' wordt verstaan, maar alle dienstverlening op afstand (zoals Cloud, SaaS, etc.).

Artikel 29. Algemeen

In het **eerste lid** is de verplichting opgenomen om alle voor hosting noodzakelijke gegevens aan de gemeente ter beschikking te stellen.

In het **tweede lid** is het recht op opschorting verder aan banden gelegd. In artikel 20.1 is al bepaald dat opschorting eerst is toegestaan na het sturen van een ingebrekestelling. De afhankelijkheid van de gemeente van de leverancier bij Hosting is veelal niettemin zo groot, dat die waarborg nog onvoldoende kan zijn. Een beroep op opschorting bij Hosting betekent immers veelal de facto het volledig frustreren van de bedrijfsvoering van de gemeente (zij kan

dan immers niet meer bij haar gegevens en/of haar software). Vandaar dat de norm voor een beroep op opschorting bij Hosting is aangescherpt.

Artikel 30. Opgeslagen gegevens

Dit artikel houdt verband met de aansprakelijkheid van leverancier voor gehoste gegevens en de wettelijke vrijwaring (artikel 6:196c BW). Uit de wet zou kunnen worden afgeleid dat de leverancier gerechtigd is gehoste gegevens prompt te verwijderen indien er een claim komt dat bepaalde informatie onrechtmatig is opgeslagen. Het artikel regelt dat het uitgangspunt is dat de gemeente eerst over dergelijke claims wordt geïnformeerd (**lid 2**) en over dergelijke claims altijd overleg met de gemeente plaatsvindt, tenzij de spoedeisendheid maakt dat dergelijk overleg niet kan worden afgewacht (**lid 3**).

Artikel 31. Onderhoud en Beschikbaarheid

Dit artikel geeft enige aanvullende bepalingen over het onderhoud van de via Hosting aangeboden ICT Prestatie. Het artikel geeft een basis beschikbaarheidslevel van 98% per maand op werkdagen tussen 08.00 en 18.00 uur (**lid 2**). In de Overeenkomst kan hier uiteraard van worden afgeweken.

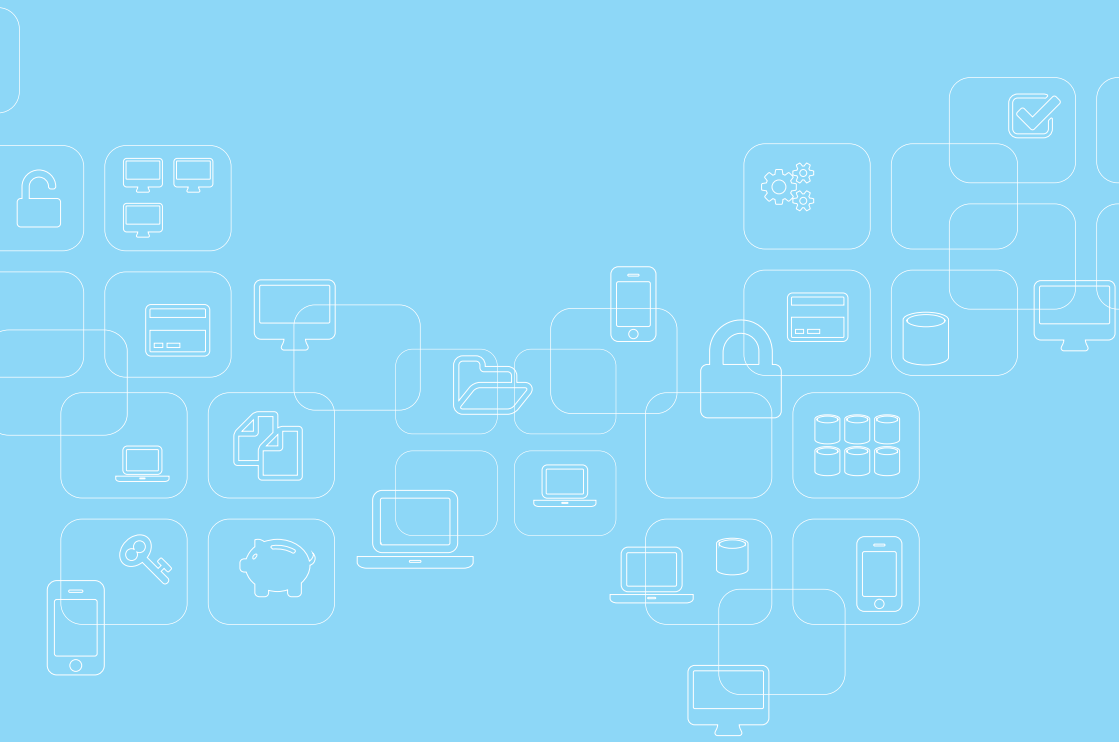
In **lid 3** is bepaald dat bij Hosting de installatie van Upgrades en Updates door de leverancier wordt verzorgd. Dit zal bij hosting veelal eigen zijn aan de aard van dienstverlening. Het artikel moet dan ook vooral worden gezien in samenhang met het bepaalde in artikel 8.10, waar juist stond dat de gemeente in beginsel zelf de installatie verzorgt (hetgeen bij hosting veelal niet mogelijk zal zijn).

In **lid 4** is bepaald dat de gemeente bij gestandaardiseerde Hosting diensten niet het recht heeft de installatie van Updates en Upgrades te weigeren. Hiermee wordt erkend dat die diensten veelal op gelijke wijze voor een veelvoud aan klanten wordt aangeboden en dat het aldus noodzakelijk is steeds mee te gaan in de ontwikkelingen die voor alle klanten gelden.

Artikel 32. Waarborgen continuïteit

Bij Hosting gelden er specifieke continuïteitsrisico's. De via de Hosting aangeboden software en de daarmee verwerkte gegevens staan immers buiten de deur. Dat betekent dat bij faillissement van de leverancier en/of diens

toeleverancier(s), de gemeente zowel in juridische als in praktische zin niet (onverkort) meer bij haar eigen data kan. **Artikel 32** erkent dit risico en bepaalt dat partijen daarover preventief, dus voordat de feitelijke faillissementssituatie zich voordoet (!), aanvullende afspraken kunnen maken. Het artikel geeft enkele voorbeelden van mogelijke afspraken die in dat kader gemaakt kunnen worden.



Colofon

UITGAVE
© **KING** Kwaliteits Instituut Nederlandse Gemeenten
www.kinggemeenten.nl

DIGITALE AGENDA 2020
Dit project draagt bij aan de Digitale Agenda 2020

VERANTWOORDING
Vastgesteld door de VNG op 8 december 2016

MEER INFORMATIE
Voor meer informatie over GIBIT kunt u de website
www.gibit.nl raadplegen

OPLAGE
3e druk, juni 2017

VORMGEVING
Studio Maartje de Sonnaville

Stadsbank Oost Nederland

Procedure Hardening

Maatregelen BIG die met deze procedure worden onderbouwd:

10.4.2.2
10.6.1.2
11.4.4.1
11.4.5.1
11.4.5.2
11.4.5.5
12.4.1.1

1.1 Doelstellingen

De Stadsbank Oost Nederland hanteert de volgende doelstellingen:

- Groepen informatiediensten, gebruikers en informatiesystemen behoren op netwerken te worden gescheiden.
- De fysieke en logische toegang tot poorten voor diagnose en configuratie behoort te worden beheerst.
- Groepen informatiediensten, gebruikers en informatiesystemen behoren op netwerken te worden gescheiden.
- Voor gemeenschappelijke netwerken, vooral waar deze de grenzen van de organisatie overschrijden, behoren de toegangsmogelijkheden voor gebruikers te worden beperkt, overeenkomstig het toegangsbeleid en de eisen van bedrijfstoepassingen.

1.2 Implementatie

De procedure beschrijft het volgende:

1. Werkstations worden zo ingericht dat routeren van verkeer tussen verschillende zones of netwerken niet mogelijk is.
2. De indeling van zones binnen de technische infrastructuur vindt plaats volgens een operationeel beleidsdocument waarin is vastgelegd welke uitgangspunten voor zonering worden gehanteerd. Van systemen wordt bijgehouden in welke zone ze staan. Er wordt periodiek, minimaal één keer per jaar, geëvalueerd of het systeem nog steeds in de optimale zone zit of verplaatst moet worden.
3. Elke zone heeft een gedefinieerd beveiligingsniveau. Zodat de filtering tussen zones is afgestemd op de doelstelling van de zones en het te overbruggen verschil in het beveiligingsniveau. Hierbij vindt controle plaats op protocol, inhoud en richting van de communicatie.
4. Beheer en audit van zones vindt plaats vanuit een minimaal logisch gescheiden, separate zone.
5. Zonering wordt ingericht met voorzieningen waarvan de functionaliteit is beperkt tot het strikt noodzakelijke (hardening van voorzieningen).
6. Poorten, diensten en soortgelijke voorzieningen op een netwerk of computer die niet vereist zijn voor de dienst dienen te worden afgesloten.
7. Netwerken zijn voorzien van beheermaatregelen voor routering gebaseerd op mechanismen ter verificatie van bron en bestemmingsadressen.

1.3 Bekendmaking

De inhoud van deze procedure moet bekend zijn bij alle medewerkers die bij deze procedure betrokken zijn.

1.4 Definities

Hardening is het proces waarbij overbodige functies in besturingssystemen uitgeschakeld worden en/of van het systeem verwijderd worden. En daarnaast door zodanige waarden toekennen aan beveiligingsinstellingen dat hiermee de mogelijkheden om een systeem te compromitteren worden verlaagd en een maximale veiligheid ontstaat. Het gaat hierbij ook om het verwijderen van niet gebruikte of onnodige gebruikers accounts, en tevens het wijzigen van standaard wachtwoorden die op sommige systemen aanwezig kunnen zijn.

Met systemen wordt in dit verband bedoeld: servers, actieve netwerkcomponenten zoals firewalls en switches, desktops, laptops, mobiele devices. Kortom, alles met een besturingssysteem. Het resultaat is een gehard systeem.

1.5 Proceseigenaar

De proceseigenaar is de manager Bedrijfsvoering en Advies.

1.6 Verantwoordelijkheid

De verantwoordelijkheid voor deze procedure ligt te allen tijde bij het dagelijks bestuur en namens deze bij de manager Bedrijfsvoering en Advies.
De verantwoordelijkheid om deze procedure toe te passen ligt bij de eigenaar van het proces waarop de hardening betrekking heeft.

1.7 Actualiteit

De proceseigenaar is verantwoordelijk voor het actueel houden van deze procedure. Indien de procedure inhoudelijk wijzigt, draagt de proceseigenaar zorg voor communicatie daarover en distributie en archivering van de procedure.

1.8 Uitvoering

[redacted]

[redacted]

12.

[redacted]

Hardening van applicaties

1.
De systeem-/netwerkbeheerder of functioneel beheerder installeert de applicatie aan de hand van de installatieprocedures van de leverancier van de desbetreffende software.

2.
De applicatie betreft altijd de meest recent uitgebrachte versie, tenzij de leverancier anders aangeeft.

3.
Als applicaties worden geleverd met een set aan vooraf gedefinieerde gebruikers- en/of administrator-accounts worden deze gecontroleerd en beoordeeld. Accounts met betrekking tot diensten of functies die niet worden gebruikt worden verwijderd of uitgeschakeld.
Voor alle standaard accounts die wel worden gebruikt, moet het standaard wachtwoord worden gewijzigd. Als het geen nadelige gevolgen heeft voor het systeem, moeten vooraf gedefinieerde accounts worden hernoemd.

4.
De rechten van standaard gebruikers worden altijd zoveel mogelijk beperkt tenzij de gebruiker specifieke rechten nodig heeft om zijn/haar taken naar behoeve uit te kunnenvoeren.

5.
Verbindingen naar of met andere applicaties waarover geclassificeerde gegevens (bijvoorbeeld persoonsgegevens) worden uitgewisseld worden uitsluitend opgezet met versleutelde verbindingen.

6.
Voorafgaand aan de installatie van een applicatie vindt een controle plaats op de virusscanner op het systeem. Er wordt gecheckt op beschikbaarheid en actualiteit.

7.
Onnodige componenten worden uitgeschakeld of verwijderd. Alle componenten die niet in productie worden gebruikt, worden uitgeschakeld of verwijderd.

8.
Het systeem waarop de applicatie draait wordt up-to-date gebracht. Alle relevante servicepacks en beveiligingspatches worden geïnstalleerd.

9.
Alle wachtwoorden voldoen aan de voorwaarden die zijn vastgelegd in het wachtwoordbeleid van de Stadsbank.

10.

Beheermogelijkheden worden zoveel mogelijk afgesloten. Webinterfaces voor beheerfuncties worden uitsluitend via beheercompartimenten (apart VLAN) en/of van vooraf gedefinieerde IP-adressen aangeboden'

Periodieke controle hardening

[redacted]

[redacted]

3.
Mede op basis van dit overzicht brengt de manager Bedrijfsvoering en Advies een rapportage uit aan het managementteam om inzicht te verschaffen in de hardening van de systemen.
In deze rapportage wordt ook melding gemaakt van eventuele door de proceseigenaar geaccepteerde afwijkingen.

Beheermaatregel:	11.4.5
Documentversie:	1.0 12 maart 2018
Documentnaam:	180312 Procedure Hardening (1.0).docx

Stadsbank Oost Nederland

Procedure Wijzigingsbeheer

Maatregelen BIG die met deze procedure worden onderbouwd:

Maatregel 6.1.4	Goedkeuringsproces voor ICT-voorzieningen
Maatregel 6.2.3	Beveiliging behandelen in overeenkomsten met een derde partij
Maatregel 10.1.2	Wijzigingsbeheer
Maatregel 10.1.4	Scheiding van faciliteiten voor ontwikkeling, testen en productie
Maatregel 10.2.3	Beheer van wijzigingen in dienstverlening door een derde partij
Maatregel 10.10.2	Controle van systeemgebruik
Maatregel 12.1.1	Analyse en specificatie van beveiligingseisen
Maatregel 12.5.1	Procedures voor wijzigingsbeheer
Maatregel 12.5.2	Technische beoordeling van toepassingen na wijzigingen in het besturingssysteem
Maatregel 12.5.3	Restricties op wijzigingen in programmatuurpakketten

1.1 Doelstellingen

In dit document wordt een beschrijving gegeven van het proces Wijzigingsbeheer. Ook wordt beschreven op welke wijze het proces is verankerd in de organisatie. Er is vooral uiteengezet welke taken, verantwoordelijkheden en bevoegdheden in het kader van het wijzigingsbeheer benodigd zijn en hoe hieraan organisatorisch invulling wordt gegeven.
Wijzigingsbeheer zorgt ervoor dat wijzigingen op de ICT-infrastructuur (ICT-middelen en - diensten) efficiënt en effectief worden doorgevoerd met zo min mogelijk verstoring van de kwaliteit van de dienstverlening, zodat deze dienstverlening blijft voldoen aan de eisen.
Bedieningsprocedures behoren te worden gedocumenteerd, bijgehouden en beschikbaar gesteld aan alle gebruikers die deze nodig hebben.

1.2 Implementatie

In de procedure voor wijzigingsbeheer is minimaal aandacht besteed aan:

- het administreren van significante wijzigingen;
- impactanalyse van mogelijke gevolgen van de wijzigingen;
- goedkeuringsprocedure voor wijzigingen.

Instellingen van informatiebeveiligingsfuncties (b.v. security software) op het koppelvlak tussen vertrouwde en onvertrouwde netwerken, moeten volgens de BIG, automatisch op wijzigingen worden gecontroleerd.

1.3 Beheerdoelstellingen

De volgende beheerdoelstellingen van wijzigingsbeheer dienen met een redelijke mate van zekerheid te worden gewaarborgd:

- Wijzigingen dienen te worden geautoriseerd met inachtneming van de risico's voor de ICT-diensten. De impact van de wijzigingen dient van tevoren op beschikbaarheids-, capaciteits-, continuïteits- en beveiligingsaspecten, evenals (eind)gebruikersaspecten te worden getoetst. Indien wijzigingen niet zijn geautoriseerd na evaluatie van de risico's, bestaat het risico dat de wijzigingen ongewenste (neven)effecten hebben op ICT-diensten, die soms niet volledig kunnen worden overzien door de initiator van de wijziging. Het is daarom van belang om deze effecten gestructureerd in kaart te brengen en de impact af te stemmen met alle belanghebbenden, zoals de eigenaar van de ICT-dienst, beheerders van ICT-middelen en de betrokkenen van andere ICT-beheerprocessen.
- Wijzigingen dienen tijdig en volledig te worden doorgevoerd. Voor het implementeren van wijzigingen dienen voldoende resources beschikbaar te zijn en de implementatie van de wijziging dient zodanig te worden gepland dat de verstoring van de dienstverlening minimaal is. Indien wijzigingen niet tijdig en volledig worden doorgevoerd, bestaat het risico dat noodzakelijke verbeteringen of de instandhouding van de ICT-diensten in het gedrang komen. Het is van belang dat wijzigingsaanvragen tijdig in behandeling worden genomen en, evenals de resulterende wijzigingen, tijdig worden afgehandeld. Daarnaast is het van belang dat, voorafgaand aan een wijziging, alle aspecten worden geïdentificeerd die eveneens een wijziging dienen te ondergaan of worden beïnvloed als gevolg van de wijziging.
- Wijzigingen dienen te worden beoordeeld op doeltreffendheid. Indien de doeltreffendheid van wijzigingen niet wordt geëvalueerd, bestaat het risico dat de wijzigingen niet, of slechts gedeeltelijk, bijdragen aan verbetering van de ICT-diensten of zelfs verstorend zijn voor de ICT-diensten. Indien wijzigingen niet het beoogde effect blijken te hebben, is het van belang om terug te kunnen keren naar de oorspronkelijke situatie (ook wel: back-out of terugvalscenario).

1.4 Bekendmaking

De inhoud van deze procedure moet bekend zijn bij alle medewerkers die bij deze procedure betrokken zijn.

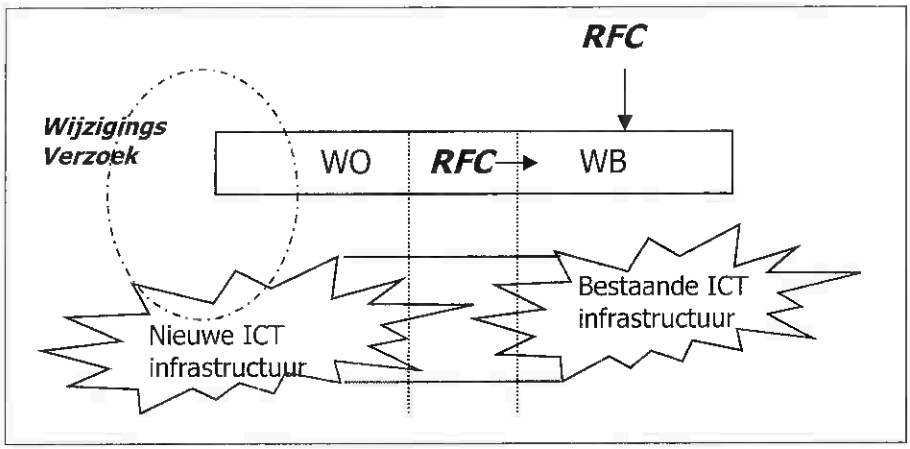
1.5 Scope

Deze procedure geldt voor alle bedrijfsapplicaties van de Stadsbank Oost Nederland.

1.6 Definities

Met de snelle technologische ontwikkelingen in de ICT zijn wijzigingen aan de orde van de dag. De ervaring leert dat het merendeel van de incidenten terug te voeren is op eerder doorgevoerde wijzigingen. Dit kan komen door onzorgvuldig werk, te krappe resources, te weinig of geen voorbereiding of testen van onvoldoende kwaliteit.
Het aantal incidenten loopt dan op en met de oplopende werkdruk is in de planning vaak geen rekening gehouden. Dit alles gaat dan weer ten koste van het geplande dagelijkse werk en het voorbereiden van andere wijzigingen.

Onderhavige procedure heeft betrekking op iedere (niet standaard) wijziging op de ICT-infrastructuur. Deze wijziging dient aangevraagd, gedocumenteerd en bewaakt te worden met een wijzigingsverzoek (= Request For Change = RFC).
Omvangrijke wijzigingen in de ICT-infrastructuur worden in principe als project opgepakt, waarbij er vanuit de Projectorganisatie (=PO) één of meerdere wijzigingsverzoeken worden ingediend bij wijzigingsbeheer (= WB). Dit gebeurt ook bij grote wijzigingen op de bestaande ICT-infrastructuur. Hieronder wordt schematisch weergegeven hoe Wijzigingsverzoeken (= RFC) binnenkomen bij Wijzigingsbeheer.



Wijziging
Een wijziging is een verandering, hoe klein ook, in de ICT infrastructuur. Aanmaken van een gebruiker is een wijziging. Het herstellen van wachtwoorden op verzoek van een eindgebruiker is ook een wijziging.

Wijzigingsverzoek (RFC)
Een formeel verzoek om een wijziging door te voeren op één of meer gespecificeerde configuratie-items.

Wijzigingsbeheerder (WB)
De wijzigingsbeheerder is verantwoordelijk voor het filteren, classificeren, accepteren, coördineren en plannen van alle wijzigingsaanvragen. Tijdens de uitvoering van wijzigingen stuurt hij het proces.

WijzigingsOverleg (WO)
Het WO is een overlegorgaan welke op vooraf geplande tijden bijeen wordt geroepen om wijzigingen te beoordelen en in te plannen. Tevens wordt hier de status van openstaande wijzigingsactiviteiten besproken. De vaste vertegenwoordigers in het WO zijn:

- de afdelingsmanager Bedrijfsvoering en Advies
- de functioneel applicatiebeheerder(s)
- de manager van het proces waarop de wijziging betrekking heeft
- de Security Officer

Het WO kan (tijdelijk) worden uitgebreid met:

- systeem/netwerkbeheerders
- IA adviseurs
- projectleiders
- externe consultants
- de CISO
- de Functionaris Gegevensbescherming

1.7 Verantwoordelijkheid

De verantwoordelijkheid voor deze procedure ligt te allen tijde bij het Dagelijks Bestuur en namens deze bij de manager Bedrijfsvoering en Advies. De verantwoordelijkheid om wijzigingsbeheer al dan niet toe te passen berust bij de proceseigenaar. De uitvoering hiervan ligt bij de Security Officer.
De verantwoordelijkheid van de leverancier bestaat er uit releasenotes aan te leveren, gecombineerd met testrapportages van nieuwe releases van de applicatie.

1.8 Proceseigenaar

De proceseigenaar is de manager Bedrijfsvoering en Advies en namens hem de security officer.

1.9 Actualiteit

De proceseigenaar is verantwoordelijk voor het actueel houden van deze procedure. Indien de procedure inhoudelijk wijzigt, draagt de proceseigenaar zorg voor communicatie daarover en verdere distributie en archivering van de procedure.

1.10 Uitvoering

[redacted]

Registratie

1.

Alle wijzigingsverzoeken worden bij binnenkomst geregistreerd.

2.
Daarna wordt gecontroleerd of:

- deze ondertekend zijn door een bevoegde;
- er kosten aan zijn verbonden: is er een grootboeknummer ingevuld.
- alle gegevens compleet zijn.

De formulieren dienen zo volledig mogelijk ingevuld te worden.

3.

Als de gegevens niet compleet zijn aangeleverd wordt contact opgenomen met de aanvrager.

4.
De wijzigingsaanvraag wordt niet eerder in behandeling genomen dan dat deze gegevens compleet zijn.

Classificeren van het wijzigingsverzoek

5.
De wijzigingsbeheerder beoordeelt alle wijzigingsverzoeken. De wijzigingsbeheerder bepaalt in eerste instantie de categorie, de impact, het traject en de prioriteit.

6
De categorie wordt bepaald op basis van impact, geld en resources. Deze classificatie bepaalt hoe de aanvraag verder zal worden behandeld.

De categorieën zijn als volgt ingedeeld:

- Routinematig. Routinematige wijzigingen zijn standaard wijzigingen welke worden uitgevoerd door de functioneel applicatiebeheerders en bewaakt worden door de wijzigingsbeheerder. Deze wijzigingen worden niet in het WO behandeld en hebben altijd een lage impact. Bijvoorbeeld het aanmaken van een nieuwe gebruiker of wijziging van een wachtwoord op verzoek van een gebruiker.

- Geringe omvang. Een wijziging met lage impact, geen financiële gevolgen en waar weinig werk mee is gemoeid. Dit wordt uitgevoerd door de functioneel applicatiebeheerders en bewaakt door de wijzigingsbeheerder. Deze wijzigingen worden niet in het WO behandeld. Bijvoorbeeld het gereed maken van een laptop voor thuisgebruik.
- Redelijke omvang. Wijzigingen met gemiddelde impact, financiële gevolgen en waar flinke inspanningen voor nodig zijn. Deze wijzigingen worden uitgevoerd door de functioneel applicatiebeheerders en bewaakt door de wijzigingsbeheerder. Deze wijzigingen worden in het WO behandeld. Bijvoorbeeld het implementeren van een nieuwe versie van programmatuur.
- Omvangrijk. Een wijziging met hoge impact, grote financiële gevolgen en waar veel werk mee is gemoeid. Deze wijzigingen worden uitgevoerd door de netwerk- of systeembeheerders in overleg met de functioneel applicatiebeheerders en bewaakt door de wijzigingsbeheerder. Deze wijzigingen worden behandeld in het WO waar eerst overeenstemming dient te zijn tussen de deelnemers voordat aan de uitvoering wordt begonnen. Bijvoorbeeld de overstap naar nieuwe programmatuur.

Impact

De impact van een wijziging is afhankelijk van de werkzaamheden die plaatsvinden op de configuratie-items van de ICT infrastructuur en de financiële gevolgen van de wijziging. De impact is als volgt ingedeeld:

- Laag. Deze wijzigingen vinden plaats op niet bedrijfskritische configuratie-items en hebben nauwelijks of geen financiële gevolgen.
- Middel. Deze wijzigingen vinden plaats op bedrijfskritische configuratie-items zonder financiële gevolgen. Of vinden plaats op niet bedrijfskritische configuratie-items met financiële gevolgen.
- Hoog. Deze wijzigingen vinden plaats op bedrijfskritische configuratie-items met financiële gevolgen.

Traject

Afhankelijk van de categorie en impact wordt bepaald welk traject de wijziging doorloopt. Er zijn twee mogelijkheden:

- Geen vooronderzoek, geen behandeling in het WO en ook geen specifieke evaluatie. Dit traject geldt voor de categorieën Routematig, geringe omvang. Deze wijzigingen hebben altijd een lage impact.
- Wel vooronderzoek en wel evaluatie. Dit traject geldt voor alle overige combinaties.
- Samen met de manager Bedrijfsvoering en Advies kan altijd besloten worden een ander traject te kiezen of een variant op bovenstaande.

Prioriteit

De prioriteit geeft het belang aan van de wijziging en wordt afhankelijk van de categorie bepaald door de wijzigingsbeheerder of het WO. De prioriteit komt tot uitdrukking in de einddatum van wijziging.

Uitvoeren van een vooronderzoek

7.

Een vooronderzoek wordt alleen uitgevoerd voor wijzigingen met de categorie "redelijke omvang" of "omvangrijk". De functioneel applicatiebeheerders gaan samen met de wijzigingsbeheerder de proces- of applicatiespecifieke onderwerpen formuleren om tot een duidelijke opdracht te komen. Deze opdracht wordt uitgewerkt in een vooronderzoek om op deze manier de wijziging te beoordelen.

8.

De wijziging wordt aan de hand van het vooronderzoek in het WO beoordeeld op:

- ICT infrastructuur;

- standaarden;
- budget;
- resources;
- etc.

9.
Als het WO positief besluit over de wijziging dan wordt deze planmatig uitgewerkt. Als het WO negatief besluit, gaat de voorgestelde wijziging niet door. Door de wijzigingsbeheerder wordt dit terug gekoppeld naar de aanvrager van de wijziging.

Uitwerking planning (analyse)

10.
Afhankelijk van de categorie van de wijziging zijn er twee mogelijkheden.

- *Categorie routinematig of geringe omvang*
- *Categorie redelijke omvang en omvangrijk.*

10a.
Wijzigingen uit de categorieën "routinematig" of "geringe omvang" worden direct uitgevoerd door de functioneel applicatiebeheerders. Ga naar stap 14 van deze procedure.

10b
Voor wijzigingen uit de categorieën "redelijke omvang" of "omvangrijk" vindt er tussen de functioneel applicatie-beheerders, de manager Bedrijfsvoering en Advies en de wijzigingsbeheerder overleg plaats om de wijziging te analyseren en een uitrolplanning te maken. Het initiatief van deze stap ligt bij de wijzigingsbeheerder. Indien gewenst door de wijzigingsbeheerder, kan de aanvrager van de wijziging deelnemen aan dit overleg.

11.
Voor wijzigingen uit de categorieën "redelijke omvang" of "omvangrijk" wordt een plan van aanpak door de wijzigingsbeheerder in overleg met de eigenaar van het te wijzigen proces opgesteld. Het plan bevat de volgende elementen:
- de verwachte inzet van de betrokken organisatie onderdelen;
- eventuele beveiligingsaspecten;
- impact van de wijziging op andere diensten;
- ICT infrastructuur;
- haalbaarheid;
- releasenotes leverancier
- testresultaten leverancier
- opgeloste bugs/openstaande bugs
- testplan;
- conflicten met andere wijzigingen.

Tevens wordt een inschatting gemaakt van de benodigde resources.

Het implementeren van een nieuwe release van een webapplicatie op de eigen infrastructuur is normaliter een omvangrijke wijziging. Het implementeren van een nieuwe release van een SAAS applicatie kan worden beschouwd als een wijziging van redelijke omvang.
Het plan van aanpak wordt door de manager Bedrijfsvoering en Advies beoordeeld op financiële haalbaarheid.

12.
Bij goedkeuring wordt de wijziging ingepland.
De goed- of afkeuring van het plan vindt enkel en alleen plaats in het WO overleg.

Coördineren
13.
Goedgekeurde wijzigingen worden doorgegeven aan de betrokken specialisten voor het doorvoeren van de wijzigingen. Met uitzondering van routinematige wijzigingen worden alle werkzaamheden verricht onder de controlerende en coördinerende rol van de wijzigingsbeheerder. Deze is immers verantwoordelijk voor de technische uitvoering van de wijziging.
Routinematige wijzigingen worden direct uitgevoerd door een ICT medewerker of een ICT beheerder.

Implementatie
14.
Afhankelijk van de categorie van de wijziging zijn er twee mogelijkheden.

- Categorie redelijke omvang en omvangrijk.
  Deze wijzigingen worden eerst in de test omgeving geplaatst waarna de applicatie wordt beoordeeld of het gebouwde voldoet aan de opdracht. Ga naar stap 15
  Hierna worden indien nodig trainingen verzorgd en de documentatie gemaakt, dan wel de door de leverancier gemaakte documentatie beoordeeld. Met de gemaakte documentatie uit de test omgeving wordt de productie omgeving ingericht.
- Categorie routinematig en geringe omvang
  Deze wijzigingen worden niet in de testomgeving geplaatst maar direct op de productie omgeving aangebracht. Hier heeft ook geen vooronderzoek plaatsgevonden. Ga naar stap 16.

Testen
15.
De wijziging wordt getest op techniek evenals op het beoogde resultaat. Bij het testen dienen in elk geval de functioneel applicatiebeheerders en afhankelijk van de situatie een gebruiker te worden betrokken. Om verder te zorgen dat het testen objectief gebeurt, is het zaak dat het testen niet door de bouwers van de wijziging wordt uitgevoerd. Ook zijn duidelijke voorschriften nodig voor het toezicht houden op de kwaliteit van het testen en van de documentatie van de testresultaten.

Implementeren
16.
Nadat het testen met succes is afgerond, kan worden begonnen met het implementeren van de wijziging in de productieomgeving.

17.
Na de implementatie van elke wijziging, wordt het verantwoordelijk management op de hoogte gesteld door de wijzigingsbeheerder.

Evaluatie

18.

Alleen de wijzigingen met categorie redelijke omvang en omvangrijk worden geëvalueerd.

De wijziging wordt geëvalueerd met de manager Bedrijfsvoering en Advies, de functioneel applicatiebeheerders, de wijzigingsbeheerder en de overige betrokken medewerkers. De evaluatie wordt op papier gezet en toegevoegd aan de documentatie.

Beheersmaatregel:	10.1.2
Documentversie:	12 maart 2018
Documentnaam:	10.1.2 Procedure Wijzigingsbeheer.docx

Stadsbank Oost Nederland

Wachtwoordbeleid Stadsbank Oost Nederland

Maatregelen BIG die met dit beleid worden onderbouwd:
Maatregel 9.1.2 (leveranciers wachtwoorden)
Maatregel 11.2.3 (beheer van wachtwoorden)
Maatregel 11.3.1 (gebruik van wachtwoorden)
Maatregel 11.5.1 (beveiligde inlogprocedures)
Maatregel 11.5.2 (gebruikers identificatie en authenticatie)
Maatregel 11.5.3 (systemen voor wachtwoordbeheer)
Maatregel 11.7.1 (draagbare computers)
Maatregel 12.1.1 (beveiligingseisen ICT-systemen)

Beleidsuitgangspunten voor het gebruik van wachtwoorden bij de Stadsbank Oost Nederland

Wachtwoorden vormen een belangrijk aspect van de informatiebeveiliging. Wachtwoorden zorgen ervoor dat onbevoegden minder makkelijk toegang kunnen krijgen tot vertrouwelijke informatie. Een gemakkelijk wachtwoord evenals onduidelijke of niet gevolgde wachtwoord procedures zijn een bedreiging voor de vertrouwelijkheid en integriteit van informatie, maar uiteindelijk ook voor het imago van de Stadsbank. Alle gebruikers van de informatiesystemen van de Stadsbank moeten goede wachtwoorden kiezen binnen de randvoorwaarden die hieraan door de Stadsbank worden gesteld en zijn verantwoordelijk voor de geheimhouding van hun wachtwoorden en inloggegevens.

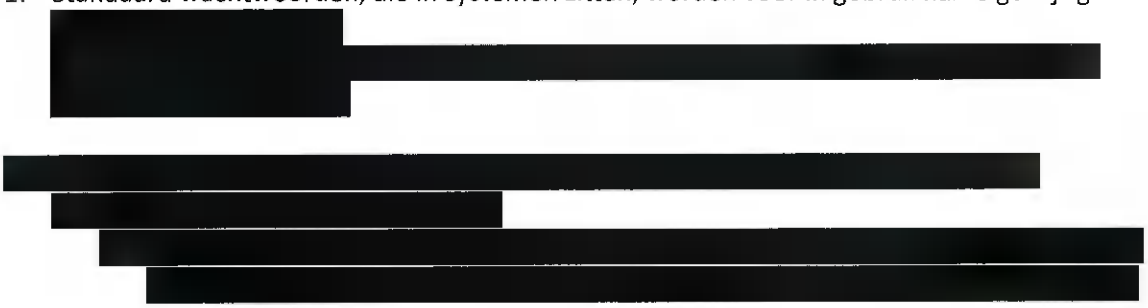
Het doel van dit wachtwoordbeleid is drieledig:

- Het vaststellen van regels waar wachtwoorden en wachtwoord procedures aan moeten voldoen.
- Het vaststellen van de bescherming van de wachtwoorden.
- Het vaststellen van de wijzigingscriteria voor wachtwoorden.

De Stadsbank hanteert de volgende beleidsuitgangspunten. Deze zijn ontleend aan de Baseline Informatiebeveiliging Gemeenten (BIG).

Algemeen beleid

1. Standaard wachtwoorden, die in systemen zitten, worden voor in gebruikname gewijzigd.



[redacted]

[redacted]

[1] Met twee-factor authenticatie wordt bedoeld : iets dat je weet (je wachtwoord) en iets dat je hebt (bijvoorbeeld een fysieke/soft token, key generator of vingerafdruk).

[redacted]

Wachtwoordbeheer

Systemen voor wachtwoordbeheer behoren interactief te zijn en moeten bewerkstelligen dat wachtwoorden van geschikte kwaliteit worden gekozen.

1. Er wordt automatisch gecontroleerd op goed gebruik van wachtwoorden (onder andere voldoende sterke wachtwoorden, regelmatige wijziging, directe wijziging van initieel wachtwoord).

2. Wachtwoorden hebben een geldigheidsduur van maximaal 60 dagen. Binnen deze tijd dient het wachtwoord te worden gewijzigd. Wanneer het wachtwoord verlopen is, wordt het account geblokkeerd.

3. Wachtwoorden die gereset zijn en initiële wachtwoorden hebben een zeer beperkte geldigheidsduur en moeten bij het eerste gebruik worden gewijzigd.

4. De gebruikers hebben de mogelijkheid hun eigen wachtwoord te kiezen en te wijzigen. Hierbij geldt het volgende:
    - Voordat een gebruiker zijn wachtwoord kan wijzigen, wordt de gebruiker opnieuw geauthenticeerd.

Rapportage en controle

[redacted]

Stadsbank Oost Nederland

VERKLARING VAN TOEPASSELIJKHEID

Versie:	0.1
Versiedatum:	13 juni 2018
Gemaakt door:	[redacted]
Vast te stellen door:	MT en Dagelijks Bestuur Stadsbank Oost Nederland

Versieblad

Datum	Versie	Gemaakt door	Omschrijving van de aanpassing
13 juni 2018	0.1	[redacted]	1e concept

Inhoudsopgave

1. Doel, toepassingsgebied en gebruikers

Het doel van dit document is om verantwoording af te leggen over de implementatie van maatregelen uit de Baseline Informatiebeveiliging Gemeenten, die passend zijn voor de Stadsbank Oost Nederland, als ook om restrisico's goed te keuren en formele goedkeuring te verkrijgen voor de implementatie van de passende maatregelen.

Uitgangspunten voor deze Verklaring van Toepasselijkheid:

- De Baseline Informatiebeveiliging Gemeenten (BIG) is de leidraad voor de inrichting van een systeem van beveiligingsmaatregelen, dat waarborgen biedt voor de beschikbaarheid, integriteit, vertrouwelijkheid en controleerbaarheid van de door de Stadsbank gebruikte informatiesystemen.
- De keuze voor de te implementeren maatregelen is gerelateerd aan de praktische toepasbaarheid van deze maatregelen in de omgeving van de Stadsbank Oost Nederland.

Dit document bevat de planning van alle beheermaatregelen vermeld in de BIG voor zover van toepassing verklaard door het MT en Dagelijks Bestuur van de Stadsbank. Deze beheermaatregelen zijn vastgelegd in het Information Security Management System (ISMS) dat wordt beheerd door de Chief Information Security Officer (CISO) .

De beveiligingsrisico's die door het MT en Dagelijks Bestuur worden geaccepteerd staan expliciet vermeld in paragraaf 4.

Gebruikers van dit document zijn alle leden van het Information Security Team (IST). Het document is raadpleegbaar voor leden van het MT.

2. Referentie documenten

- Strategische Baseline Informatiebeveiliging Gemeenten, versie 1.02
- Tactische Baseline Informatiebeveiliging Gemeenten, versie 1.02
- 180301 Informatiebeveiligingsbeleid SON (versie 2018)

3. Toepasselijkheid van beheermaatregelen

De Tactische Baseline Informatiebeveiliging Nederlandse Gemeenten is het normenkader dat de beschikbaarheid, integriteit en exclusiviteit van gemeentelijke informatie(systemen) bevordert. Deze Tactische Baseline is een normenkader die een totaalpakket aan informatiebeveiligingsmaatregelen omvat die voor iedere gemeente geldt. Deze Tactische Baseline is opgezet rondom bestaande normen; de NEN/ISO 27002:2007 en NEN/ISO 27001:2005. Deze standaarden zijn voor de Nederlandse overheid gekozen en algemeen aanvaard als de norm voor informatiebeveiliging.

In onderstaande tabel worden de verschillende aandachtsgebieden (domeinen) van de BIG beschreven, de doelstelling van dit aandachtsgebied in relatie tot informatiebeveiliging en de getroffen maatregelen.

Domein	Doelstelling	Belangrijkste maatregelen
Beveiligingsbeleid	Borgen van betrouwbare dienstverlening en een aantoonbaar niveau van informatiebeveiliging dat voldoet aan de relevante wetgeving, algemeen wordt geaccepteerd door haar (keten-)partners en er mede voor zorgt dat de kritische bedrijfsprocessen bij een calamiteit en incident voortgezet kunnen worden.	
Organisatie van de informatiebeveiliging	Beheren van de informatiebeveiliging binnen de organisatie.	
Beheer van bedrijfsmiddelen	Bereiken en handhaven van een adequate bescherming van bedrijfsmiddelen van de organisatie.	
Personele beveiliging	Bewerkstelligen dat werknemers, ingehuurd personeel en externe gebruikers hun verantwoordelijkheden begrijpen, en geschikt zijn voor de rollen waarvoor zij worden overwogen, en om het risico van diefstal, fraude of misbruik van faciliteiten te verminderen.	
Fysieke beveiliging	Het voorkomen van onbevoegde fysieke toegang tot, schade aan of verstoring van het terrein en de informatie van de organisatie.	
Beheer van communicatie- en bedieningsprocessen	Waarborgen van een correcte en veilige bediening van ICT-voorzieningen.	

Domein	Doelstelling	Belangrijkste maatregelen
Logische toegangsbeveiliging	Beheersen van de toegang tot informatie	[redacted]
Verwerving, ontwikkeling en onderhoud van informatiesystemen	Bewerkstelligen dat beveiliging integraal deel uitmaakt van informatiesystemen.	
Beheer van beveiligingsincidenten	Bewerkstelligen dat informatiebeveiligingsgebeurtenissen en zwakheden die verband houden met informatiesystemen zodanig kenbaar worden gemaakt dat tijdig corrigerende maatregelen kunnen worden genomen.	[redacted]
Bedrijfscontinuïteitsbeheer	Tegengaan van onderbreking van bedrijfsactiviteiten en bescherming van kritische bedrijfsprocessen tegen de gevolgen van omvangrijke storingen in informatiesystemen of rampen en om tijdig herstel te bewerkstelligen.	[redacted]
Naleving	Voorkomen van schending van enige wetgeving, wettelijke en regelgevende of contractuele verplichtingen, en van enige beveiligingseisen	[redacted]

De Stadsbank Oost Nederland heeft voor de inrichting van de beveiligingsorganisatie de 133 verschillende beheermaatregelen en de 303 hierop gebaseerde beveiligingsmaatregelen van de BIG als uitgangspunt gehanteerd. De BIG is niet als uitputtende checklist gebruikt, maar als kader voor een op de organisatie van de Stadsbank passende beveiligingsorganisatie.

In het Information Security Management System (ISMS) is de toepasselijkheid en status van alle maatregelen vastgelegd. Een aantal maatregelen is door het IST beoordeeld als niet noodzakelijk, omdat het met deze maatregelen weg te nemen risico te gering wordt beschouwd ten opzichte van de kosten die aan het treffen van de maatregelen verbonden zijn. Deze geaccepteerde risico's worden hierna aangegeven. Het ISMS fungeert tevens als beheertool voor de actualiteit van de maatregelen en het monitoren van afspraken over uit te voeren acties.

4. Geaccepteerde risico's

Onderstaande beheermaatregelen zijn opgenomen in de BIG maar zullen niet door de Stadsbank worden geïmplementeerd omdat de risico's die gelopen worden, worden geaccepteerd omdat:

- de kans op het optreden van het risico als verwaarloosbaar wordt ingeschat;
- en/of de impact (de mogelijke schade) als aanvaardbaar wordt gezien;
- en/of de kwetsbaarheid verlagende maatregel als te kostbaar wordt ingeschat.

Nr.	Beheermaatregel uit de BIG	Eigenaar	Toelichting
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]

Nr.	Beheermaatregel uit de BIG	Eigenaar	Toelichting

5. Geldigheid en documentbeheer

Dit document is geldig vanaf de datum van vaststelling. De eigenaar van dit document is de CISO. Hij controleert jaarlijks de actualiteit van de beveiligingsmaatregelen en rapporteert hierover aan MT en Dagelijks Bestuur, als onderdeel van de P&C-cyclus.

Aldus vastgesteld door het Dagelijks Bestuur van de Stadsbank Oost Nederland op .

_____

[handtekening]

Uitzondering Art 5.1 lid 2 onder e
en h WOO

Van : [redacted]
Aan : IST-team
Datum : 25 juli 2018
Betreft: verslag Privacy Impact Assessment Beschermingsbewind

---

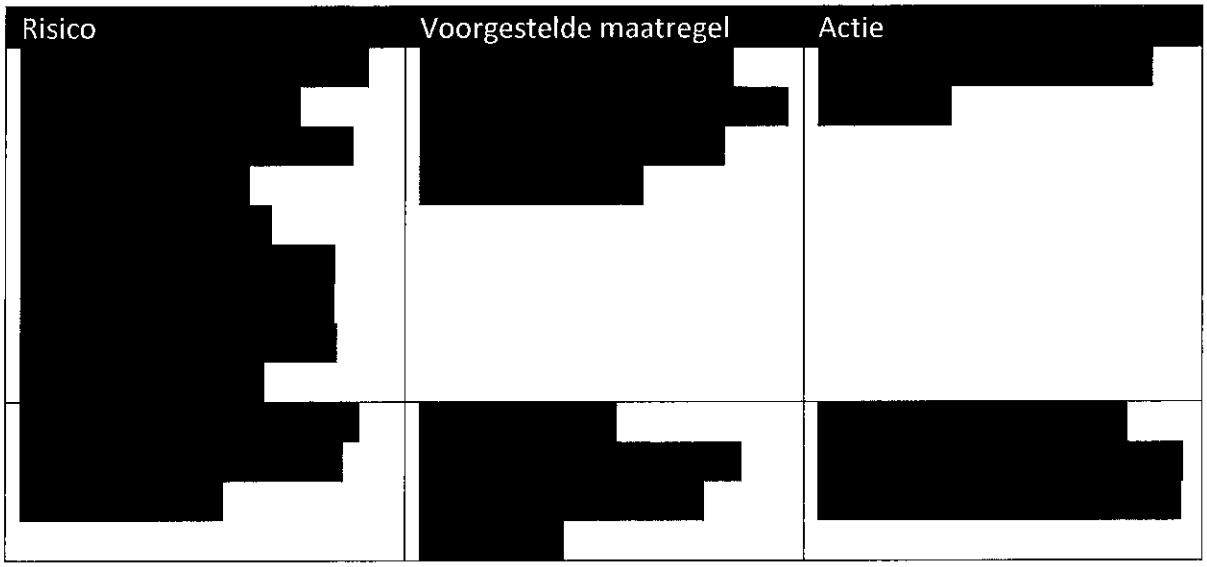
Inleiding
Op 11 juli jl. is een onderzoek uitgevoerd op basis van interviews om te bepalen of er risico's verbonden zijn aan het waarborgen van de vertrouwelijkheid van persoonsgegevens in het proces Beschermingsbewind. De interviews zijn afgenomen door [redacted] De geinterviewden zijn [redacted] Aanleiding voor het uitvoeren van dit onderzoek is een wezenlijke wijziging in de uitvoering van werkzaamheden, namelijk de overgang van Allegro naar SmartFMS als gegevensverwerkend systeem.

Scope van het onderzoek
De PIA richt zich op het proces beschermingsbewind en het ondersteunende systeem SmartFMS. Beschermingsbewind is één van de primaire taken van de Stadsbank Oost Nederland. Daarom wordt het proces geclassificeerd als een strategisch proces. Bij de verwerking van persoonsgegevens worden de volgende risicogebieden onderscheiden:
- verzamelen van gegevens
- gebruik van gegevens
- bewaren en vernietigen van gegevens
- beveiliging van de gegevens

Gesignaleerde risico's

Risico	Voorgestelde maatregel	Actie
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]


Risico
Voorgestelde maatregel
Actie



Vervolg

De verantwoordelijke lijnmanager moet een beoordeling maken van de wenselijkheid om de voorgestelde maatregelen te treffen ten opzichte van de impact van die maatregel op het werkproces. Er is een aantal manieren om met de genoemde risico's om te gaan, namelijk:

- het risico wordt geaccepteerd omdat de kans dat het risico zich voordoet klein wordt geacht en/of de gevolgschade gering is;
- het risico wordt vermeden door de werkwijze zodanig aan te passen dat het risico verdwijnt;
- het risico wordt verminderd door het treffen van aanvullende beveiligingsmaatregelen;
- het risico wordt overgedragen aan een andere partij, bijvoorbeeld een verzekeringsmaatschappij.

Afspraken ten aanzien van de gesignaleerde risico's moeten worden vastgelegd. Het verslag hiervan moet worden opgeslagen in het ISMS.

Stadsbank Oost Nederland

VERKLARING VAN TOEPASSELIJKHEID 2019

Versie:	0.1
Versiedatum:	3 mei 2019
Gemaakt door:	[redacted]
Vast te stellen door:	MT en Dagelijks Bestuur Stadsbank Oost Nederland

Versieblad

Datum	Versie	Gemaakt door	Omschrijving van de aanpassing
3 mei 2019	0.1	[redacted]	1e concept

Inhoudsopgave

1. Doel, toepassingsgebied en gebruikers

Het doel van dit document is om verantwoording af te leggen over de implementatie van maatregelen uit de Baseline Informatiebeveiliging Gemeenten, die passend zijn voor de Stadsbank Oost Nederland, als ook om restrisico's goed te keuren en formele goedkeuring te verkrijgen voor de implementatie van de passende maatregelen.

Uitgangspunten voor deze Verklaring van Toepasselijkheid:

- De Baseline Informatiebeveiliging Gemeenten (BIG) is de leidraad voor de inrichting van een systeem van beveiligingsmaatregelen, dat waarborgen biedt voor de beschikbaarheid, integriteit, vertrouwelijkheid en controleerbaarheid van de door de Stadsbank gebruikte informatiesystemen.
- De keuze voor de te implementeren maatregelen is gerelateerd aan de praktische toepasbaarheid van deze maatregelen in de omgeving van de Stadsbank Oost Nederland.

Dit document bevat de planning van alle beheermaatregelen vermeld in de BIG voor zover van toepassing verklaard door het MT en Dagelijks Bestuur van de Stadsbank. Deze beheermaatregelen zijn vastgelegd in het Information Security Management System (ISMS) dat wordt beheerd door de Chief Information Security Officer (CISO) .

De beveiligingsrisico's die door het MT en Dagelijks Bestuur worden geaccepteerd staan expliciet vermeld in paragraaf 4. Ten opzichte van 2018 zijn hierin geen wijzigingen opgetreden. De BIG gaat in 2020 over in de Baseline Informatiebeveiliging Overheid (BIO). Vanaf 2020 zal de 'Verklaring van Toepasselijkheid' conform de BIO worden verantwoord. Het jaar 2019 vormt een overgangsjaar, waarin de maatregelen van de BIG uit 2018 worden gecontinueerd en er een omzetting plaatsvindt van de BIG naar de BIO.

Gebruikers van dit document zijn alle leden van het Information Security Team (IST). Het document is raadpleegbaar voor leden van het MT.

2. Referentie documenten

- Strategische Baseline Informatiebeveiliging Gemeenten, versie 1.02
- Tactische Baseline Informatiebeveiliging Gemeenten, versie 1.02
- 180301 Informatiebeveiligingsbeleid SON (versie 2018)

3. Toepasselijkheid van beheermaatregelen

De Tactische Baseline Informatiebeveiliging Nederlandse Gemeenten is het normenkader dat de beschikbaarheid, integriteit en exclusiviteit van informatie(systemen) van gemeenten en verbonden partijen bevordert. Deze Tactische Baseline is een normenkader die een totaalpakket aan informatiebeveiligingsmaatregelen omvat. Deze Tactische Baseline is opgezet rondom bestaande normen; de NEN/ISO 27002:2007 en NEN/ISO 27001:2005. Deze standaarden zijn voor de Nederlandse overheid gekozen en algemeen aanvaard als de norm voor informatiebeveiliging.

In onderstaande tabel worden de verschillende aandachtsgebieden (domeinen) van de BIG beschreven, de doelstelling van dit aandachtsgebied in relatie tot informatiebeveiliging en de getroffen maatregelen.

Domein	Doelstelling	Belangrijkste maatregelen
Beveiligingsbeleid	Borgen van betrouwbare dienstverlening en een aantoonbaar niveau van informatiebeveiliging dat voldoet aan de relevante wetgeving, algemeen wordt geaccepteerd door haar (keten-)partners en er mede voor zorgt dat de kritische bedrijfsprocessen bij een calamiteit en incident voortgezet kunnen worden.	Vastgesteld informatiebeveiligingsbeleid.
Organisatie van de informatiebeveiliging	Beheren van de informatiebeveiliging binnen de organisatie.	Vaststellen taken, bevoegdheden en verantwoordelijkheden binnen de beveiligingsorganisatie.
Beheer van bedrijfsmiddelen	Bereiken en handhaven van een adequate bescherming van bedrijfsmiddelen van de organisatie.	Inventarisatie van bedrijfsmiddelen, vastleggen van het eigenaarschap en regels voor gebruik. Classificatie van informatie (Stadsbank hanteert voor alle in gebruik zijnde gegevens de classificatie "Vertrouwelijk").


Domein
Doelstelling
Belangrijkste maatregelen

Domein	Doelstelling	Belangrijkste maatregelen
[redacted]	[redacted]	[redacted]

De Stadsbank Oost Nederland heeft voor de inrichting van de beveiligingsorganisatie de 133 verschillende beheermaatregelen en de 303 hierop gebaseerde beveiligingsmaatregelen van de BIG als uitgangspunt gehanteerd. De BIG is niet als uitputtende checklist gebruikt, maar als kader voor een op de organisatie van de Stadsbank passende beveiligingsorganisatie.

In het Information Security Management System (ISMS) is de toepasselijkheid en status van alle maatregelen vastgelegd. Een aantal maatregelen is door het IST beoordeeld als niet noodzakelijk, omdat het met deze maatregelen weg te nemen risico te gering wordt beschouwd ten opzichte van de kosten die aan het treffen van de maatregelen verbonden zijn. Deze geaccepteerde risico's worden hierna aangegeven. Het ISMS fungeert tevens als beheertool voor de actualiteit van de maatregelen en het monitoren van afspraken over uit te voeren acties.

4. Geaccepteerde risico's

Onderstaande beheermaatregelen zijn opgenomen in de BIG maar zullen niet door de Stadsbank worden geïmplementeerd omdat de risico's die gelopen worden, worden geaccepteerd omdat:

- de kans op het optreden van het risico als verwaarloosbaar wordt ingeschat;
- en/of de impact (de mogelijke schade) als aanvaardbaar wordt gezien;
- en/of de kwetsbaarheid verlagende maatregel als te kostbaar wordt ingeschat.

Nr.	Beheermaatregel uit de BIG	Eigenaar	Toelichting
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]

Nr.	Beheermaatregel uit de BIG	Eigenaar	Toelichting
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]

Nr.	Beheermaatregel uit de BIG	Eigenaar	Toelichting
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]

5. Geldigheid en documentbeheer

Dit document is geldig vanaf de datum van vaststelling. De eigenaar van dit document is de CISO. Hij controleert jaarlijks de actualiteit van de beveiligingsmaatregelen en rapporteert hierover aan MT en Dagelijks Bestuur, als onderdeel van de P&C-cyclus.

Aldus vastgesteld door het Dagelijks Bestuur van de Stadsbank Oost Nederland op 26 juni 2019,

_____

[handtekening]

Stadsbank Oost Nederland

Verslag DPIA Fundaments

Januari 2020

Verslag DPIA Fundaments

Inleiding

Op 7 januari 2020 is een Data Protection Impact Assessment (DPIA) uitgevoerd om te bepalen of er risico's verbonden zijn aan het waarborgen van de vertrouwelijkheid van persoonsgegevens in het wijzigen van leverancier van hosting en back-up. Het onderzoek is uitgevoerd door [redacted] Aanleiding voor het uitvoeren van dit onderzoek is een aanzienlijke verandering in de uitvoering van werkzaamheden, namelijk de overgang van [redacted]. Tevens heeft er een interview plaatsgevonden met een materiedeskundige ([redacted], Junior IT-medewerker). Het interview is afgenomen door [redacted]

Scope van het onderzoek

De DPIA richt zich op de overgang naar een andere leverancier van hosting en back-up van alle gegevens van de Stadsbank Oost Nederland. Na een vereiste aanbesteding is er gekozen voor een andere leverancier, namelijk [redacted] Door deze overgang worden alle gegevens van de Stadsbank overgezet naar andere servers. Daarom wordt de wijziging geclassificeerd als een aanzienlijke verandering in de verwerking van persoonsgegevens. Bij de verwerking van persoonsgegevens worden de volgende risicogebieden onderscheiden:

- verzamelen van gegevens
- gebruik van gegevens
- bewaren en vernietigen van gegevens
- beveiliging van de gegevens

Gesignaleerde risico's

Risico	Voorgestelde maatregel	Actie
[redacted]	[redacted]	[redacted]

Risico	Voorgestelde maatregel	Actie
[redacted]		
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]

Vervolg

De verantwoordelijke lijnmanager moet een beoordeling maken van de wenselijkheid om de voorgestelde maatregelen te treffen ten opzichte van de impact van die maatregel op het werkproces. Er is een aantal manieren om met de genoemde risico's om te gaan, namelijk:

- het risico wordt geaccepteerd omdat de kans dat het risico zich voordoet klein wordt geacht en/of de gevolgschade gering is;
- het risico wordt vermeden door de werkwijze zodanig aan te passen dat het risico verdwijnt;
- het risico wordt verminderd door het treffen van aanvullende beveiligingsmaatregelen;
- het risico wordt overgedragen aan een andere partij, bijvoorbeeld een verzekeringsmaatschappij.

Afspraken ten aanzien van de gesignaleerde risico's moeten worden vastgelegd. Het verslag hiervan moet worden opgeslagen in het ISMS.

Calamiteitenplan Stadsbank Oost Nederland

Versie: 2.0, 28-02-2023
Auteur: [redacted]

Inhoudsopgave

1 Algemeen

1.1 Inleiding

Om de taken van de Stadsbank uit te kunnen voeren zijn processen in bedrijf die als 'kritisch' worden aangemerkt. Dit betekent dat langdurige uitval van deze bedrijfsprocessen vanwege de negatieve gevolgen voor de Stadsbank, haar klanten, medewerkers, en andere betrokkenen onacceptabel is. Om langdurige stagnatie van de kritische bedrijfsprocessen van de Stadsbank te voorkomen moet een proces voor continuïteitsbeheer worden ingericht. Onderdeel van dit proces vormt het opstellen van het calamititeitenplan. In dit plan zijn de acties vastgelegd die moeten worden uitgevoerd, nadat een calamiteit is ontstaan.

Alle medewerkers, in het bijzonder degenen die een rol hebben binnen dit calamiteitenplan, moeten op de hoogte zijn van hetgeen van hen wordt verwacht in geval van een calamiteit. Daarvoor wordt dit calamiteitenplan regelmatig getest. Dit draagt ertoe bij dat de noodzakelijke stappen om de voortgang van de bedrijfsprocessen te waarborgen zo snel en efficiënt mogelijk worden genomen na het optreden van een calamiteit.

1.2 Crisisbeheer

Crisisbeheer is gericht op het zo snel en effectief mogelijk beperken van de effecten en het wegnemen van de bron van de calamiteit.
De procedure voor het in werking stellen van het calamiteitenplan is beschreven net zoals de taken en verantwoordelijkheden van functionarissen, teams en organisatieonderdelen. Ook de bedrijfsprocessen die tijdens een calamiteit niet mogen uitvallen zijn beschreven. De procedure voor het informeren en mobiliseren van doelgroepen en derden moet beschreven zijn evenals de benodigde middelen. De contactgegevens van alle doelgroepen, interne en externe diensten en derden moeten ook in het calamiteitenplan worden opgenomen.

1.3 Wat is ons doel en onze doelgroep

Dit calamiteitenplan beschrijft de acties die moeten worden uitgevoerd, nadat een calamiteit heeft plaatsgevonden die de voortgang van kritische bedrijfsprocessen in gevaar brengt. Als gevolg daarvan komt de dienstverlening van de Stadsbank in gevaar. De aanleiding kan een stroomstoring zijn waardoor ICT, energievoorzieningen en huisvesting niet meer of maar gedeeltelijk functioneren. Maar ook zonder stroomstoring kan de ICT van de Stadsbank uitvallen (bijvoorbeeld als gevolg van een cyberaanval) met allerlei mogelijke gevolgen.

Het doel van dit calamiteitenplan is om de effecten van een calamiteit zoveel mogelijk te reduceren, de dienstverlening te continueren en het herstel te bespoedigen. Hierbij kan onderscheid worden gemaakt in activiteiten in de voorbereidingsfase en de fase dat daadwerkelijk een calamiteit heeft plaatsgevonden.
Ter voorbereiding moet de Stadsbank een aantal maatregelen treffen om (nood)voorzieningen te organiseren. Deze (nood)voorzieningen moeten het functioneren van de kritische bedrijfsprocessen in geval van uitval opvangen – althans voor een bepaalde periode.

Tijdens een calamiteit moet een aantal activiteiten worden ondernomen om de continuïteit van de dienstverlening in stand te houden of te herstellen en de effecten zo snel en effectief mogelijk te beperken.

De doelgroep van dit calamiteitenplan zijn de medewerkers die bij uitval belast zijn met het zoveel mogelijk reduceren van de effecten van een calamiteit, het continueren van de bedrijfsprocessen en de voorbereiding op uitval. Op bestuurlijk niveau is dat het Dagelijks Bestuur, op tactisch/operationeel niveau is dat de manager Bedrijfsvoering en Advies, met ondersteuning vanuit het Information Security Team (IST-team) en medewerkers met expertise op het gebied van facilitaire zaken (zoals ICT inclusief telefonie/ andere communicatiemiddelen, gebouwenbeheer en beveiliging).

1.4 Afbakening en reikwijdte

Het calamiteitenplan beschrijft de acties die uitgevoerd moeten worden, nadat een calamiteit heeft plaatsgevonden die zodoende de voortgang van de kritische bedrijfsprocessen in gevaar brengt. Het calamiteitenplan heeft alleen betrekking op de waarborging van de voortgang van de bedrijfsprocessen. Het calamiteitenplan besteedt dus geen aandacht aan ontruiming, redding en schadebeperking direct na het optreden van een calamiteit. Die aspecten zijn onderdeel van het ontruimingsplan.

1.5 Definitie 'calamiteit'

Een calamiteit wordt in het kader van dit plan gedefinieerd als een ongewenste gebeurtenis die zodanige negatieve gevolgen heeft dat de voortgang van de kritische bedrijfsprocessen wordt verstoord en de maximale uitvalsduur van deze kritische bedrijfsprocessen dreigt te worden overschreden.

1.6 Beschrijving bedrijfsprocessen

Onderstaande bedrijfsprocessen van de Stadsbank worden als kritische bedrijfsprocessen beschouwd:
- Schuldhulpverlening
- Beschermingsbewind
- Kredieten

[redacted]

De kans op systeemuitval wordt verwaarloosbaar klein geacht door de redundante opzet van de ondersteunende systemen (servers en databases).

1.7 Wat zijn onze uitgangspunten

Bij het opstellen van dit plan is de dienstverlening van de Stadsbank het startpunt. De dienstverlening omvat een aantal kritische en niet-kritische bedrijfsprocessen. De uitvoerbaarheid daarvan is afhankelijk van beschikbare middelen (bijvoorbeeld menskracht, ICT of transportmiddelen en huisvesting). Deze middelen kunnen door externe factoren (ofwel risico's) geraakt worden (bijvoorbeeld een grieppandemie met uitval van menskracht tot gevolg, een stroomstoring met effect op ICT). De impact op de beschikbaarheid van middelen zal verschillen en daarmee ook op de uitvoering van de kritische bedrijfsprocessen.

Met andere woorden: de uitvoering van een kritisch bedrijfsproces is afhankelijk van middelen die bij een calamiteit mogelijk wegvallen. In dit plan wordt beschreven wat wordt georganiseerd om de impact van de uitval van middelen zo veel mogelijk te verkleinen en de kritische bedrijfsprocessen te continueren. Het gaat enerzijds om de maatregelen (noodvoorzieningen). Anderzijds betreft het de inrichting van een crisisstructuur om snel en adequaat te kunnen reageren als een calamiteit zich voordoet (bijvoorbeeld de uitval van elektriciteit en/of ICT).

1.8 Verantwoordelijkheden continuïteitsplan

De manager Bedrijfsvoering en Advies is verantwoordelijk voor de inhoud en actualiteit van het calamiteitenplan. De Security Officer is verantwoordelijk voor het beheer van het plan. In het kader van beheer vindt een jaarlijkse toetsing van het calamiteitenplan plaats.
Na het optreden van een calamiteit wordt het IST-team bij elkaar geroepen. Het IST-team is verantwoordelijk voor de uitvoering van de activiteiten tijdens een calamiteit.

1.9 Inhoud continuïteitsplan

Dit calamiteitenplan bevat de volgende onderdelen. In hoofdstuk 2 is de organisatie van continuïteitsbeheer vastgelegd. Hoofdstuk 3 beschrijft de afhankelijkheden om de continuïteit van bedrijfsprocessen te garanderen. Hoofdstuk 4 beschrijft de wijze van activering van het calamiteitenplan. In hoofdstuk 5 zijn de gegevens opgenomen die tijdens een calamiteit beschikbaar moeten zijn en de bereikbaarheidsgegevens van zowel interne als externe betrokkenen.

2 Organisatie continuïteitsbeheer

2.1 Toelichting

In geval van een calamiteit wordt veelal gewerkt onder hoge druk. In een korte tijd moeten veel beslissingen worden genomen, die grote gevolgen kunnen hebben. Op grond van deze kenmerken wordt tijdens een calamiteit vaak volgens een afwijkende organisatie dan in de normale situatie gewerkt.

2.2 Crisisorganisatie

De Stadsbank moet beschikken over een structuur voor incident- of crisisbeheer. De crisisorganisatie moet beschikken over toereikend mandaat om het calamiteitenplan in werking te stellen en maatregelen uit te voeren. De crisisorganisatie moet onder de directe verantwoordelijkheid van het Dagelijks Bestuur opereren.
De crisisorganisatie moet de samenstelling op basis van de kenmerken van de calamiteit aanpassen om de benodigde expertise te mobiliseren.
Binnen de crisisorganisatie moet onderscheid gemaakt worden tussen het IST-team en de overige betrokkenen binnen de Stadsbank.

De taken en verantwoordelijkheden van de mensen die een rol spelen bij de besluitvorming, het verdelen van taken, of het bijstaan in de uitvoering van het calamiteitenplan, moeten vastgelegd zijn.

2.3 Crisisbeheerteam

Het crisisbeheerteam moet de volgende taken en verantwoordelijkheden hebben:
- het nemen van alle besluiten die noodzakelijk zijn voor een zo goed mogelijke continuering van de kritische bedrijfsprocessen
- het coördineren van de activiteiten in het kader van continuiteitsherstel
- het coördineren van de timing van alle activiteiten
- het toezicht houden op de uitvoering van de activiteiten
- het onderhouden van contacten met alle interne betrokkenen bij de afhandeling van de calamiteit
- het informeren van het direct betrokken medewerkers
- het er voor zorgdragen dat alle activiteiten inzake de afhandeling van de calamiteit schriftelijk worden vastgelegd, zodat een evaluatie mogelijk is.

Het crisisbeheerteam moet de volgende bevoegdheden hebben:
- het nemen van alle beslissingen die nodig zijn voor een zo spoedig mogelijke en verantwoorde hervatting van de kritische bedrijfsprocessen
- het betreden van alle locaties die op enigerlei wijze van belang zijn voor de hervatting van de kritische bedrijfsprocessen
- het doen van mededelingen aan de betrokkenen.

Expertise	Verantwoordelijke	Taken
[redacted]	[redacted]	[redacted]

In paragraaf 5.2 zijn de bereikbaarheidsgegevens van de leden van het crisisbeheerteam (met name het IST-team) opgenomen.

2.4 Lijnmanagers

Taken en verantwoordelijkheden van de lijnmanagers zijn bijvoorbeeld:

- het uitvoeren van de activiteiten die noodzakelijk zijn voor een zo goed mogelijke continuering van de kritische bedrijfsprocessen
- het informeren van het crisisbeheerteam van de voortgang van de herstelactiviteiten.
- Et cetera.

De overige betrokkenen hebben bijvoorbeeld de volgende bevoegdheden:

- het betreden van alle locaties die op enigerlei wijze van belang zijn voor de hervatting van de kritische bedrijfsprocessen met waarborging van de eigen veiligheid
- het doen van mededelingen aan het crisisbeheerteam over de voortgang van de herstelactiviteiten.
- Et cetera.

Expertise	Verantwoordelijke	Taken
Schuldhulpverlening	Manager dienstverlening	Bewaken voortgang herstelactiviteiten
Beschermingsbewind	Manager beschermingsbewind	Bewaken voortgang herstelactiviteiten
Kredieten	Manager beschermingsbewind	Bewaken voortgang herstelactiviteiten

In paragraaf 5.2 zijn de bereikbaarheidsgegevens van de overige betrokkenen opgenomen.

2.5 Informeren

De inwerkingstelling van het calamiteitenplan kan een directe impact hebben op de continuïteit van bijvoorbeeld (keten)partners en de samenleving. De inwerkingstelling van het calamiteitenplan moet dan ook gecommuniceerd worden aan alle doelgroepen. Hiervoor moet de communicatiemedewerker gebruik maken van de bereikbaarheidsgegevens in paragraaf 7.2. Continuïteitsbeheer

2.6 Toelichting

In de continuïteitsstrategie dient in geval van een calamiteit vastgesteld te zijn welke maatregelen er getroffen zijn om de continuïteit van de kritische bedrijfsprocessen te garanderen.

3 Activering calamiteitenplan

3.1 Toelichting

Na het ontstaan van een calamiteit moet het calamiteitenplan in werking worden gesteld. Dit moet zo snel mogelijk gebeuren, zodat de noodzakelijke acties tijdig kunnen worden gestart. Voor kritische bedrijfsprocessen met een hoge beschikbaarheid hoeft voor het inwerking stellen van het herstelscenario niet gewacht te worden op de activering van het gehele calamiteitenplan volgens de hierna beschreven procedures. De dienstdoende manager van het team dat verantwoordelijk is voor de voortgang van het getroffen bedrijfsproces is bevoegd om direct na het optreden van een calamiteit de noodzakelijke acties voor het waarborgen van de kritische onderdelen van het bedrijfsproces in werking te stellen. Na activering van het gehele calamiteitenplan moet het crisisbeheerteam zo spoedig mogelijk contact opnemen met de dienstdoende leidinggevende om de acties af te stemmen en te coördineren. Er moet onderscheid worden gemaakt naar de activering van het calamiteitenplan tijdens en buiten kantooruren.

3.2 Activering calamiteitenplan

Alarmering en opschaling van de crisisorganisatie moet plaatsvinden volgens de vaste structuur én criteria die de Stadsbank daarvoor heeft opgesteld. In het geval van een serieus te nemen (dreigende) calamiteit, moet het calamiteitenplan geactiveerd worden, met als doel om de bedrijfsprocessen te ondersteunen die nodig zijn om de doelstellingen van de Stadsbank te behalen.
Het plan kan als geheel in werking gesteld worden bij een continuïteitsverstoring. Er moet vastgelegd worden welke medewerkers het plan in werking kunnen stellen en onder welke omstandigheden, voorwaarden en in overleg met wie, het plan geactiveerd kan worden.

De activering van het calamiteitenplan kan bijvoorbeeld volgens de volgende stappen plaatsvinden:

1. Na het ontstaan van de calamiteit neemt de medewerker contact op met zijn lijnmanager. Hierbij dient rekening gehouden te worden met:
   - Hoe wordt de uitval/calamiteit van opgemerkt?
   - Wie krijgt melding en hoe van de uitval/calamiteit?
2. De lijnmanager neemt contact op met de manager Bedrijfsvoering en Advies.
3. De manager Bedrijfsvoering en Advies bepaalt op grond van de melding of het Information Security Team (IST-team) wordt gealarmeerd.
4. Als het IST-team wordt gealarmeerd, wordt contact opgenomen met de security officer en de CISO.
5. Het IST-team bepaalt op grond van de beschikbare informatie binnen hoeveel tijd het calamiteitenplan wordt geactiveerd.
6. Wanneer het calamiteitenplan wordt geactiveerd, worden alle in het plan opgenomen en gezien de aard van de calamiteit relevante betrokkenen gewaarschuwd.

4 Algemene gegevens

4.1 Toelichting

Dit hoofdstuk bevat een aantal algemene gegevens die tijdens een calamiteit beschikbaar moeten zijn.

4.2 Beschrijving continuïteitsvoorzieningen

Binnen de Stadsbank wordt na het optreden van een calamiteit gebruik gemaakt van de [redacted]

4.3 Distributielijst calamiteitenplan

Hieronder wordt weergegeven welke functionarissen een kopie van het calamiteitenplan moeten ontvangen. Daarnaast wordt het calamiteitenplan voor de medewerkers van de Stadsbank op het intranet (Plek) gepubliceerd.

Functie
Manager Bedrijfsvoering en Advies
Managers Dienstverlening
Security Officer
CISO
Functionaris Gegevensbescherming
Communicatieadviseur

5 Bereikbaarheidsgegevens

5.1 Toelichting

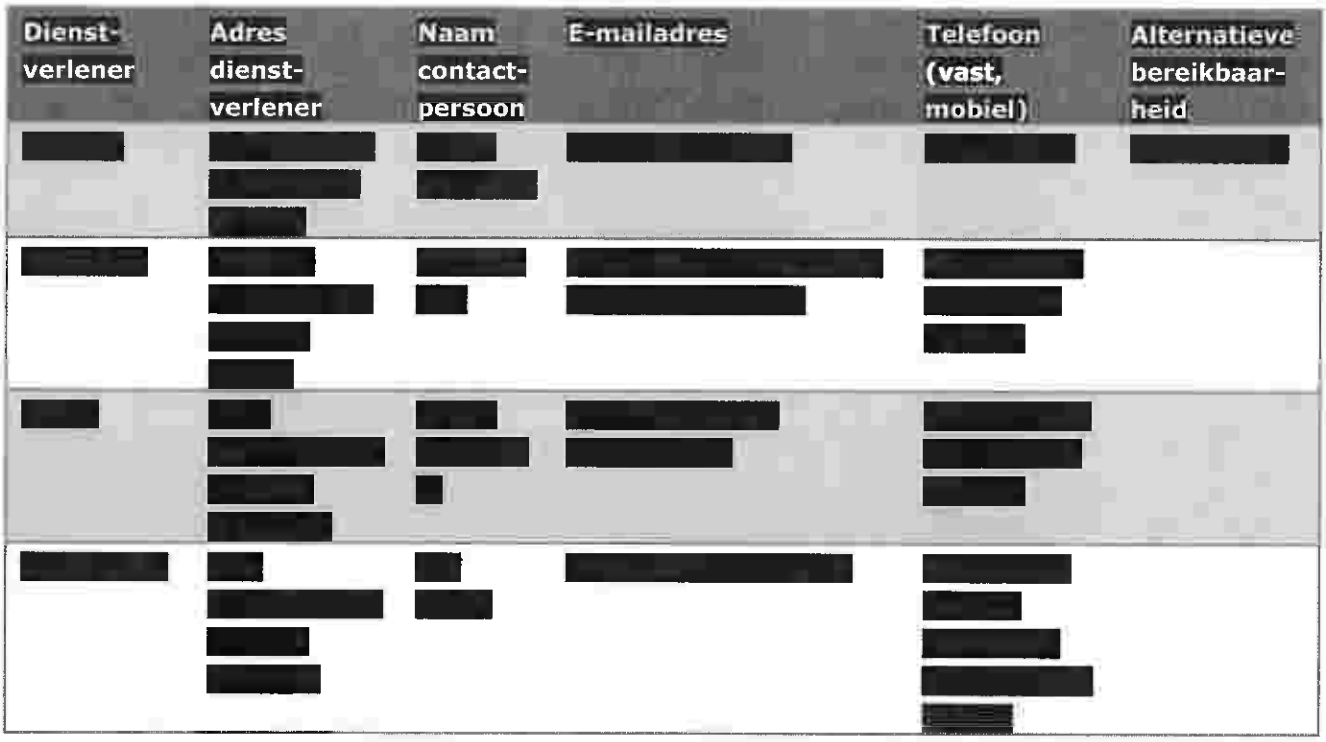
In dit hoofdstuk worden de bereikbaarheidsgegevens van alle interne en externe diensten, organisaties en dienstverleners die van belang zijn voor de continuïteit van de Stadsbank opgenomen.

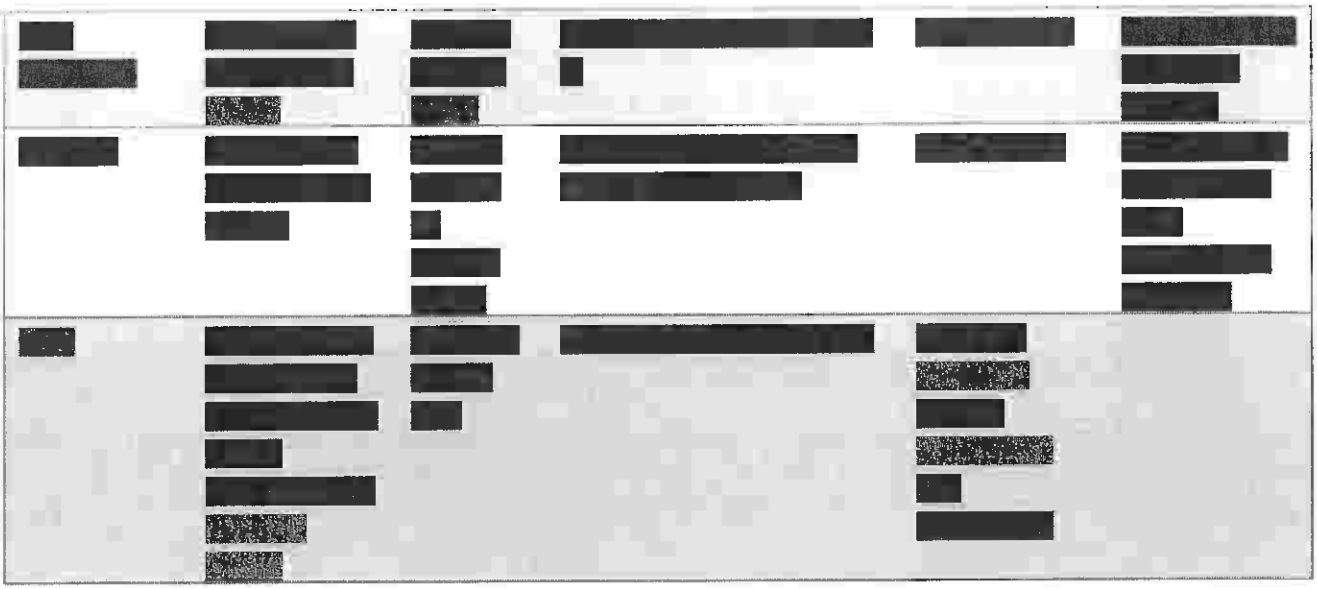
5.2 Bereikbaarheidsgegevens interne betrokkenen

Bereikbaarheidsgegevens IST-team en overige betrokkenen binnen de Stadsbank.

5.3 Bereikbaarheidsgegevens externe betrokkenen

Bereikbaarheidsgegevens externe betrokkenen, zoals leveranciers en externe (keten)partners.





DPIA	*Invullen nieuwe soort verwerking/nieuwe applicatie/nieuw project*	Toelichting
1. Welke persoonsgegevens worden verwerkt?	☑ Naam ☑ Adres ☑ Postcode ☑ Woonplaats ☑ E-malladres ☑ Telefoonnummer ☑ Geboortedatum ☑ Leeftijd ☑ Huwelijkse status ☑ Geslacht ☑ Opleiding ☑ Financiële gegevens ☑ Kentekengegevens ☐ Ras of etniciteit ☐ Politieke opvattingen ☐ Religieuze of levensbeschouwelijke overtuigingen ☐ Lidmaatschap van een vakbond ☐ Gegevens over iemands seksuele gedrag of seksuele gerichtheid ☑ Door de overheid uitgegeven identificatienummers, bijvoorbeeld BSN ☐ Kopieën van identiteitsbewijzen, zoals rijbewijs of paspoort ☑ Strafrechtelijke gegevens ☑ Medische gegevens (gezondheid) ☐ Overige	*Vul de toelichting zo volledig mogelijk in. Dit scheelt veel werk in het vervolgtraject en maakt het eenvoudiger om de DPIA te beoordelen door de FG.*
2. Korte omschrijving van het nieuwe soort verwerking/nieuwe applicatie/nieuw project:		
3. Korte schets van de gegevensstroom die hierdoor gaat plaatsvinden:	Allegro -> Xential -> Quadient -> klant/instantie/schuldeiser -> DMS JOIN	

	Toelichting	Vul in: ja/nee	Opmerkingen:
5. Is er (naast de AVG) veel wet- en regelgeving ten aanzien van persoonsgegevens waar rekening mee gehouden moet worden bij deze nieuwe verwerking?	Houd bij de beantwoording rekening met: 1. Sectorale wetgeving 2. Gedragscodes 3. Algemene maatregelen van bestuur 4. Jurisprudentie 5. Internationale aspecten	nee	zie jaarlijks verslag aan Dagelijks Bestuur 'Financiële Rechtmatigheid en Risicomanagement'.
6. Worden er zo weinig mogelijk gegevens verzameld?	Zijn de gegevens die worden verzameld allemaal nodig voor het doel?	ja	

7. Worden de gegevens met derden (interne en/of externe partijen) gedeeld?	Houd bij de beantwoording rekening met: 1. Afdelingen die gebruikmaken van de gegevens 2. Afdelingen die de gegevens verzamelen 3. De personen die toegang hebben tot de gegevens	nee	
8. Worden de gegevens gedeeld met landen buiten de EER?	Bij de EER horen de EU-lidstaten en Noorwegen, IJsland en Liechtenstein.	nee	
9. Worden de gegevens verzameld op basis van één van de wettelijke grondslagen?	De grondslagen voor het verwerken van gegevens worden in art. 6 van de AVG genoemd: 1. De gegevens worden verwerkt op basis van toestemming 2. De gegevens worden verwerkt, omdat het noodzakelijk is voor de uitvoering van een overeenkomst waarbijd e betrokkene een partij is 3. De gegevens worden verwerkt, omdat het nodig is voor een wettelijke verplichting 4. De betrokkene heeft er een vitaal belang bij dat de gegevens verzameld worden 5. De gegevens worden verwerkt, omdat ze nodig zijn zijn voor de goede vervulling van een publiekrechtelijke taak 6. De gegevens worden verwerkt, omdat daar een gerechtvaardigd belang voor is	ja	zie verwerkingsregister
10. Weet de betrokkene van deze verwerking?		ja	zie Privacy statement. Gegevensverwerking is nodig om doel (Schuldhulpverlening) te realiseren
11. Is de impact van de verwerking op de betrokkene groot?		nee	gegevens zijn noodzakelijk om dienst uit te voeren en wordt niet openbaar.
12. Is de kwaliteit van de gegevens gewaardborgd, dat wil zeggen: zijn de gegevens volledig, juist en actueel?		ja	Worden altijd realtime uit Aliegro gehaald.
13. Worden de gegevens breed verspreid binnen de organisatie?	Houd bij beantwoording rekening met: 1. Welke afdelingen toegang hebben tot de gegevens 2. Welke personen toegang hebben tot de gegevens 3. De doelen en het gebruik van de gegevens	nee	alleen medewerkers met juiste authorisatie kunnen bij gegevens.
14. Is er een bewaartermijn voor de gegevens vastgesteld?	Houd hierbij rekening met het doel waarvoor de gegevens zijn verzameld en vervolgens worden verwerkt, en bedrijfsrichtlijnen en wettelijk vastgestelde bewaartermijnen bijvoorbeeld in de Archiefwet.	Ja	
15. Worden de gegevens na verstrijken van de bewaartermijn op een dusdanige manier vernietigd of verwijderd dat ze niet meer te benaderen en te gebruiken zijn?	Houd hierbij rekening met: 1. Of regelgeving of beleid bestaat voor vernietiging van gegevens (bijvoorbeeld Archiefwet) 2. Waar (welke locatie) gegevens worden bewaard 3. Op welk medium (papier, CD, harde schijf) gegevens worden bewaard 4. O f deze locatie/medium zijn afgeschermd voor gebruik 5. Welke andere redenen bestaan om de gegevens te bewaren zoals bedrijfshistorische, wettelijke, juridische redenen	ja	
16. Is duidelijk op welke wijze aan de gestelde eisen in het beveiligingsbeleid voldaan gaan worden?	Denk hierbij aan welke maatregelen getroffen worden om te voldoen aan het beschreven beleid (een informatiebeveiligingsplan)	ja	Zie informatiebeveiligingsbeleid en tool ISMS.
Ingevuld door:			
Datum invulling:	14-12-2020		
Handtekening:			
	Datum: 17-12-2020	Paraaf:	

Stadsbank
Oost Nederland

Verslag DPIA Data B

Januari 2024

Verslag DPIA Data B

Inleiding

Op 22 januari 2024 is een Data Protection Impact Assessment (DPIA) uitgevoerd om te bepalen of er risico's verbonden zijn aan het waarborgen van de vertrouwelijkheid van persoonsgegevens in het wijzigen van leverancier van postverwerking. Het onderzoek is uitgevoerd door [redacted]).
Aanleiding voor het uitvoeren van dit onderzoek is een aanzienlijke verandering in de uitvoering van werkzaamheden, namelijk de overgang van Docuwork naar Data B als leverancier van postverwerking. Tevens heeft er informatie-uitwisseling plaatsgevonden met een materiedeskundige ([redacted]

Scope van het onderzoek

De DPIA richt zich op de overgang naar een andere leverancier van postverwerking van de Stadsbank Oost Nederland. Na een vereiste aanbesteding is er gekozen voor een andere leverancier, namelijk Data B. Door deze overgang worden alle ontvangen fysieke poststukken en de ontvangen e-mails van ca. 35 algemene inboxen van de Stadsbank gescand en gekenmerkt door een andere leverancier. Daarom wordt de wijziging geclassificeerd als een aanzienlijke verandering in de verwerking van persoonsgegevens. Bij de verwerking van persoonsgegevens worden de volgende risicogebieden onderscheiden:

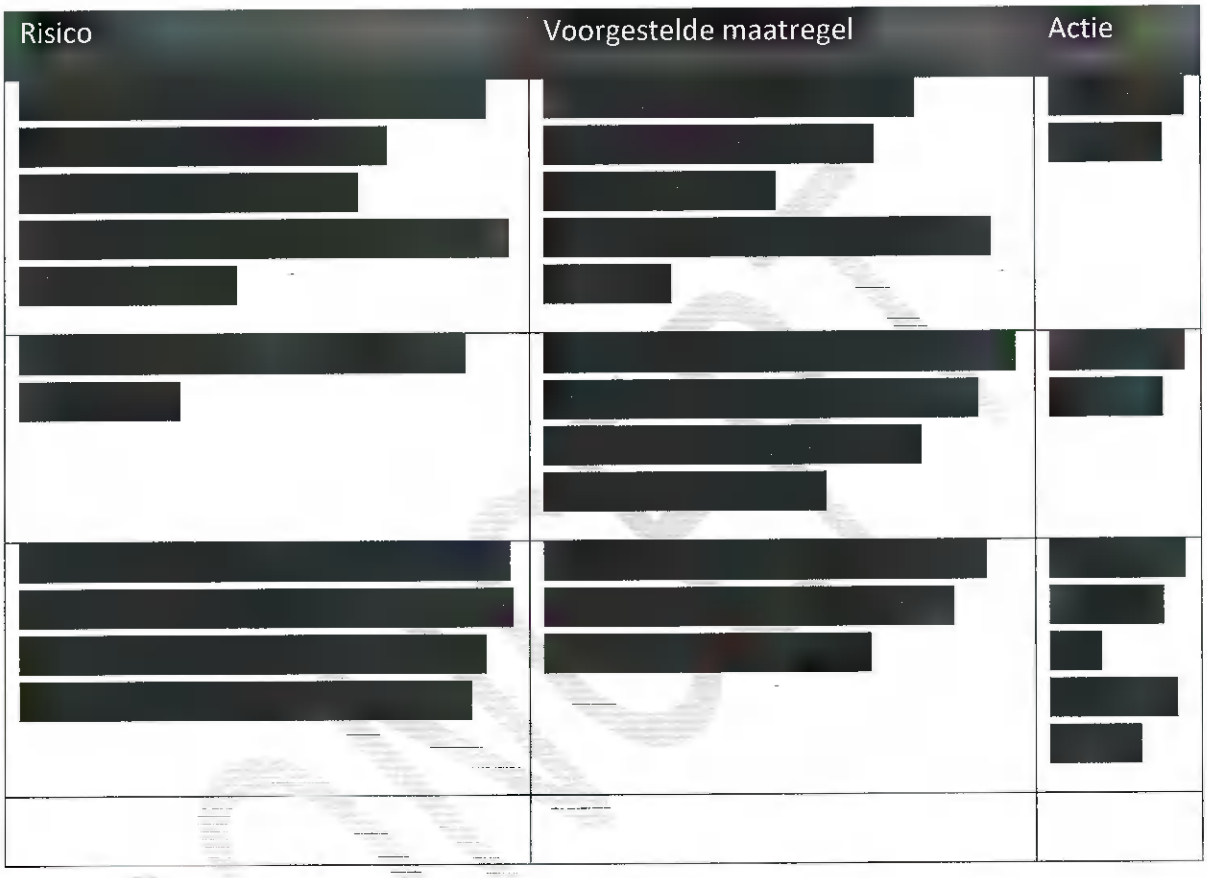
- verzamelen van gegevens
- gebruik van gegevens
- bewaren en vernietigen van gegevens
- beveiliging van de gegevens

Korte schets gegevensstroom

Fysieke poststukken worden bij Data B afgeleverd door PostNL (middels een doorzendservice) en door SON. Dit wordt gescand. Data B leest ook emailboxen van SON uit. Met behulp van AI worden poststukken en emails ingelezen om te bepalen welk documenttype het betreft en vergeleken met een database om te bepalen in welke poststroom het document moet komen. De output wordt op een netwerklocatie klaargezet en daarmee is de verwerking beëindigd. De hiervoor beschreven databases

zijn tabellen met onder meer klantgegevens op een beveiligde netwerklocatie van SON. Data B heeft (met de nodige inloggegevens) toegang tot deze locatie en leest deze documenten dagelijks uit. Na het einde van de verwerking wordt de fysieke post korte tijd (ca. 3 maanden) opgeslagen bij Data B en daarna vernietigd.

Gesignaleerde risico's



Vervolg

De manager Bedrijfsvoering en Advies moet een beoordeling maken van de wenselijkheid om de voorgestelde maatregelen te treffen ten opzichte van de impact van die maatregel op het werkproces. Er zijn een aantal manieren om met de genoemde risico's om te gaan, namelijk:

- het risico wordt geaccepteerd omdat de kans dat het risico zich voordoet klein wordt geacht en/of de gevolgschade gering is;
- het risico wordt vermeden door de werkwijze zodanig aan te passen dat het risico verdwijnt;
- het risico wordt verminderd door het treffen van aanvullende beveiligingsmaatregelen;
- het risico wordt overgedragen aan een andere partij, bijvoorbeeld een verzekeringsmaatschappij.

Afspraken ten aanzien van de gesignaleerde risico's moeten worden vastgelegd. Het verslag hiervan moet worden opgeslagen in het ISMS.

Wat: Mailbeveiliging
Van: IST
Waarom? AVG

Tel tot drie voor je klantgegevens via mail verstuurt!

We hebben de vraag al een keer gesteld tijdens de lunchsessies over informatiebeveiliging en privacy en we herhalen hem nog eens:

Is het écht noodzakelijk dat je klantgegevens toevoegt aan je e-mail? Uitgangspunt is dat we het verzenden van vertrouwelijke informatie via de mail willen voorkomen. Welke informatie valt hier precies onder?

- BSN
- E-mailadres
- Financiele gegevens
- Gezondheidsgegevens
- Enz.

Daar kunnen we ons werkproces vaak op inrichten. Moet je toch persoonsgegevens verzenden via e-mail? Dan is er de verplichting om de e-mail beveiligd te verzenden.

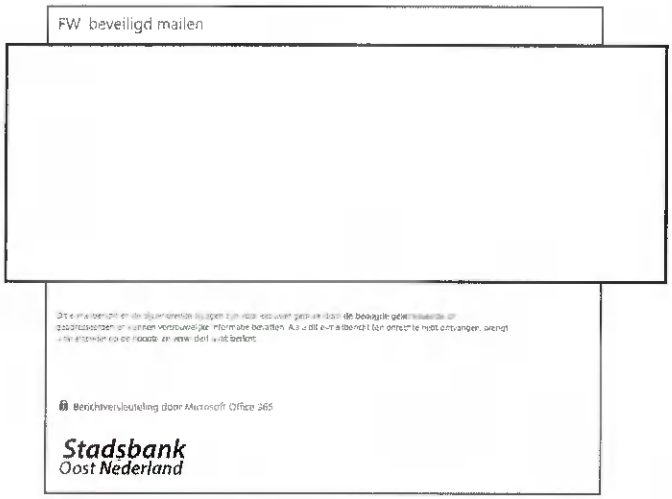
Hoe doe je dat?
Als je een e-mail met persoonsgegevens wilt versturen, moet je het woord "safe" of "beveiligd" in de onderwerp-regel van je bericht zetten. Er mogen daarnaast ook andere woorden in het onderwerp staan.

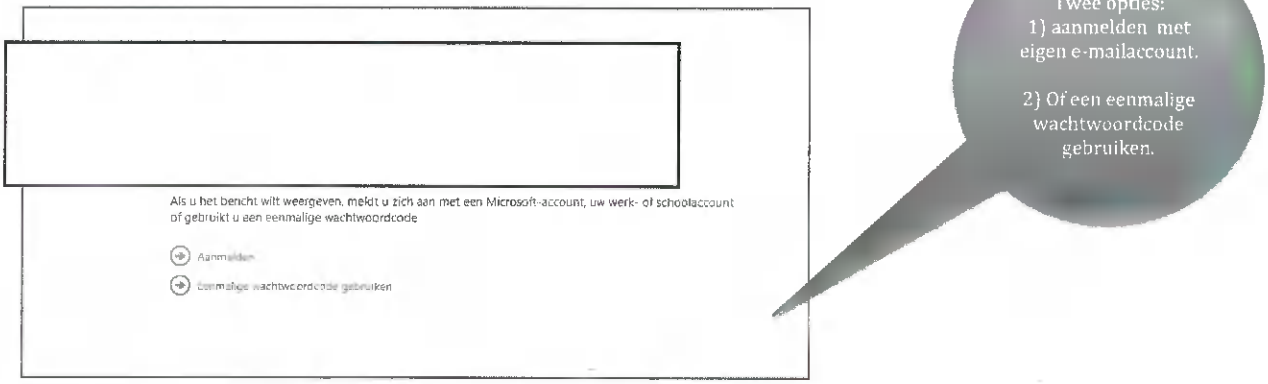
Hoe weet je of het werkt?
Test het door jezelf een e-mail te sturen, dan zie je ook welk bericht de ontvanger krijgt. Aan dit ontvangstbericht wordt een instructie toegevoegd, als het gaat om 'hoe' de e-mail te openen.

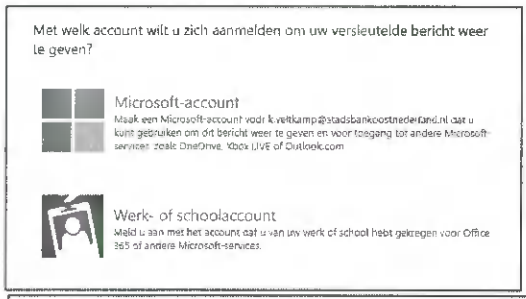
Welke stappen zijn er bij het versleuteld versturen van e-mails?
Bekijk de schermafbeeldingen op de volgende pagina, ter illustratie. Let op: dit document is intern gericht en het is NIET de bedoeling dat je het deelt met derden omdat in het voorbeeld bestaande e-mailadressen zijn gebruikt.

>>>

Hierbij een aantal schermafbeeldingen ter illustratie (op volgorde)



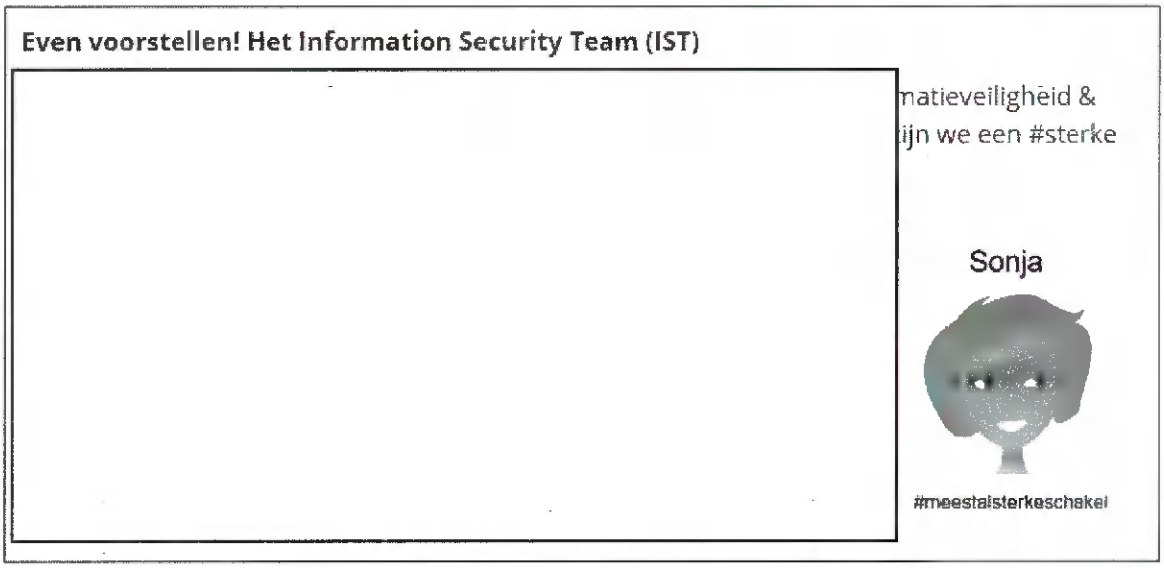




Let op: zet e-mail bewust in als het gaat om klantgegevens delen
Deze instructie geldt voor die gevallen, waarin je het verzenden van klantgegevens niet kunt vermijden. Dus tel altijd eerst tot drie om jezelf even de tijd te geven hierover na te denken.

Want, wat zou jij ervan vinden als jouw persoonsgegevens worden verstuurd dóór iemand anders náár iemand anders, zonder dat je er erg in hebt?

Heb je vragen over het versleuteld versturen van e-mails (encrypted messages) ? Neem contact op met Matthijs.



Uitzondering Art 5.1 lid 2 onder e WOO

DPIA	Invullen nieuwe soort verwerking/nieuwe applicatie/nieuw project	Toelichting
1 Welke persoonsgegevens worden verwerkt?	☑ Naam ☑ Adres ☑ Postcode ☑ Woonplaats ☑ E-mailadres ☑ Telefoonnummer ☑ Geboortedatum ☑ Leeftijd ☑ Huwelijkse status ☑ Geslacht ☑ Opleiding ☑ Financiële gegevens ☑ Kentekengegevens ☑ Ras of etniciteit ☑ Politieke opvattingen ☑ Religieuze of levensbeschouwelijke overtuigingen ☑ Lidmaatschap van een vakbond ☑ Gegevens over iemands seksuele gedrag of seksuele gerichtheid ☑ Door de overheid uitgegeven identificatienummers, bijvoorbeeld BSN ☑ Kopieën van identiteitsbewijzen, zoals rijbewijs of paspoort ☑ Strafrechtelijke gegevens ☑ Medische gegevens (gezondheid) ☐ Overige	*Het betreft de verwerking van document(en (fysieke post)stukken en email(s) van klanten van Stadsbank Oost Nederland, van derden, en voor/medewerker(s) van Stadsbank Oost Nederland zelf. Dit in het kader van de diensten (o.a. beschermingsbewind, budgetbeheer, schulden regelen en kredieten verstrekken) die SON verricht*
	Een korte beschrijving om welke gegevens het gaat:	
2. Korte omschrijving van het nieuwe soort verwerking/nieuwe applicatie/nieuw project:	**Data 8 gaat (als vervanger van de vorige postverwerker) fysieke poststukken voor ons digitaliseren en toekennen aan een registratie/dossier in JOIN. Dit geldt ook voor emails die ontvangen worden in de emailboxen die door meerdere medewerkers van de SON samen worden gebruikt (ca 35 emailadressen).**	
3. Korte schets van de gegevensstroom die hierdoor gaat plaatsvinden:	**Fysieke poststukken worden bij Data 8 afgeleverd door PostNL (middels een doorzendservice) en door SON. Dit wordt ingescand. Data 8 leest ook emailboxen van SON uit. Met behulp van AI worden poststukken en emails ingelezen om te bepalen werk documenttype het betreft, en vergeleken met een database om te bepalen in welke poststroom het document moet komen. De output wordt op een netwerklocatie klaargezet en daarmee is de verwerking beeindigd. De hiervoor beschreven databases zijn tabellen met ondermeer klantgegevens op een beveiligde netwerklocatie van SON. Data 8 heeft (met de nodige inloggegevens) toegang tot deze locatie en leest deze documenten dagelijks uit. Na het einde van de verwerking wordt de fysieke post**	
	Toelichting	**Vul in: ja/nee**	**Opmerkingen:**
5. Is er (naast de AVG) veel wet- en regelgeving ten aanzien van persoonsgegevens waar rekening mee gehouden moet worden bij deze nieuwe verwerking?	Houd bij de beantwoording rekening met: 1. Sectorale wetgeving 2. Gedragscodes 3. Algemene maatregelen van bestuur 4 Jurisprudentie 5. Internationale aspecten	[redacted]	Nee, enkel WGS, Wft en WWFT.
6 Worden er zo weinig mogelijk gegevens verzameld?	Zijn de gegevens die worden verzameld allemaal nodig voor het doel?	[redacted]	Er wordt enkel data verzameld die van belang is voor de uitvoering van de dienstverlening van SON.
7 Worden de gegevens met derden (interne en/of externe partijen) gedeeld?	Houd bij de beantwoording rekening met: 1. Afdelingen die gebruikmaken van de gegevens 2. Afdelingen die de gegevens verzamelen 3 De personen die toegang hebben tot de gegevens	[redacted]	
8. Worden de gegevens gedeeld met landen buiten de EER?	Bij de EER horen de EU-lidstaten en Noorwegen, IJsland en Liechtenstein.	[redacted]	

9. Worden de gegevens verzameld op basis van een van de wettelijke grondslagen?	De grondslagen voor het verwerken van gegevens worden in art. 6 van de AVG genoemd: 1. De gegevens worden verwerkt op basis van toestemming 2. De gegevens worden verwerkt, omdat het noodzakelijk is voor de uitvoering van een overeenkomst waarbij e betrokkene een partij is 3. De gegevens worden verwerkt, omdat het nodig is voor een wettelijke verplichting 4. De betrokkene heeft er een vitaal belang bij dat de gegevens verzameld worden 5. De gegevens worden verwerkt, omdat ze nodig zijn voor de goede vervulling van een publiekrechtelijke taak 6. De gegevens worden verwerkt, omdat daar een gerechtvaardigd belang voor is	1a	Gegevens worden in de voorfase verwerkt op grond van 6. Voor de uitvoering van diensten wordt gegevens verwerkt op grond van 2 (schulden oplossen, budgetbeheer en kredietverstrekking) en 3 (beschermingsbewind)
10. Weet de betrokkene van deze verwerking?		1b	
11. Is de impact van de verwerking op de betrokkene groot?		Nee	
12. Is de kwaliteit van de gegevens gewaarborgd, dat wil zeggen: zijn de gegevens volledig, juist en actueel?		Ja	
13. Worden de gegevens breed verspreid binnen de organisatie?	Houd bij beantwoording rekening met: 1. Welke afdelingen toegang hebben tot de gegevens 2. Welke personen toegang hebben tot de gegevens 3. De doelen en het gebruik van de gegevens	Nee	De verwerking eindigt nadat Data 8 de poststukken op een netwerklocatie heeft gezet. Deze locatie is enkel toegankelijk voor ICT medewerkers van SGN.
14. Is er een bewaartermijn voor de gegevens vastgesteld?	Houd hierbij rekening met het doel waarvoor de gegevens zijn verzameld en vervolgens worden verwerkt, en bedrijfsrichtlijnen en wettelijk vastgestelde bewaartermijnen bijvoorbeeld in de Archiefwet	Ja	De klaargezette poststukken op de netwerklocatie worden direct na het inlezen (in JOIN) geautomatiseerd verwijderd. Met Data 8 moet nog worden afgestemd dat de fysieke post na 3 maanden wordt verwijderd.
15. Worden de gegevens na verstrijken van de bewaartermijn op een dusdanige manier vernietigd of verwijderd dat ze niet meer te benaderen en te gebruiken zijn?	Houd hierbij rekening met: 1. Of regelgeving of beleid bestaat voor vernietiging van gegevens (bijvoorbeeld Archiefwet) 2. Waar (welke locatie) gegevens worden bewaard 3. Op welk medium (papier, CD, harde schijf) gegevens worden bewaard 4. Of deze locatie/medium zijn afgeschermd voor gebruik 5. Welke andere redenen bestaan om de gegevens te bewaren (zoals bedrijfshistorische, wettelijke, juridische redenen	Ja	De klaargezette poststukken op de netwerklocatie worden direct na het inlezen (in JOIN) geautomatiseerd verwijderd. Met Data 8 moet nog worden afgestemd dat de fysieke post na 3 maanden wordt verwijderd.
16. Is duidelijk op welke wijze aan de gestelde eisen in het beveiligingsbeleid voldaan gaan worden?	Denk hierbij aan welke maatregelen getroffen worden om te voldoen aan het beschreven beleid (zoer informatiebeveiligingsplan)	Ja	Conform BIO (SOM) en certificering Data 8 (ISO 27001:2013)

Ingevuld door:

Datum invulling:

Handtekening:

[redacted]

Datum: 22-01-2024

Stadsbank Oost Nederland

Postadres: Postbus 1393
7500 BJ Enschede

Bezoekadres: Spelbergsweg 35-37
7512 DX

Contact: T: 088 - 766 3666
E: info@stadsbankoostnederland.nl
W: www.stadsbankoostnederland.nl

Bankrekening: 151568464
IBAN: NL22RABO0151568464
BIC: RABONL2U

KvK-nummer: 50830953

Btw-nummer: NL0032.57.812.B.01

Ons kenmerk:	Uw kenmerk:	Afdeling:	Datum:
WOO verzoeken - 25-00001		Directie	21-08-2025

Behandeld door:	Telefoonnummer:
I.F. Walhof	088 - 7663710

Betreft: Besluit op uw verzoek in het kader van de Wet open overheid

Geachte

U heeft op 15 juli 2025 een verzoek op grond van de Wet open overheid gestuurd. In deze brief nemen wij een besluit op uw verzoek.

Juridisch kader
Iedereen mag aan een bestuursorgaan zoals de Stadsbank Oost Nederland, vragen om documenten openbaar te maken volgens de Wet open overheid (hierna noemen we deze wet: Woo). Een vraag om het openbaar maken van documenten noemen wij een Woo-verzoek.

Het uitgangspunt is dat alle overheidsinformatie openbaar is. Soms zijn er redenen om bepaalde informatie niet openbaar te maken. In hoofdstuk 5 van de Woo staan deze redenen genoemd. Wij beoordelen of er een uitzonderingsgrond van toepassing is. Wij delen bijvoorbeeld géén persoonlijke informatie, zoals namen en e-mailadressen en informatie die betrekking heeft op mogelijke kwetsbaarheden in ons geautomatiseerde systeem en maatregelen om te voorkomen dat er van deze kwetsbaarheden gebruik kan worden gemaakt -door o.a. onbevoegden- waardoor er schade kan ontstaan -in de meest brede zin van het woord- bij onze organisatie en/of klanten die van de dienstverlening van onze organisatie afhankelijk zijn. Daarbij denken wij in het bijzonder aan hackers die deze informatie kunnen misbruiken.

Uw verzoek
Op 15 juli 2025 ontvingen wij van u het volgende verzoek: "Ik verzoek om openbaarmaking voor eenieder van informatie die uw organisatie onder zich heeft op het gebied van haar eigen AVG-compliancy in de periode van 2018 tot heden. Hieronder versta ik onder meer AVG-implementatiedocumenten, de in deze periode gemaakte impactanalyses voor de gegevensverwerking (PIA/DPIA), AVG-
impactanalyses bij aanbestedingen, algemeen AVG-beleid ten aanzien van gegevens van medewerkers en andere betrokkenen, et cetera.
Ik verzoek u mijn Woo-verzoek binnen de daarvoor geldende termijn te beantwoorden.
Ik verzoek u per e-mail met mij te corresponderen."

Op 13 augustus 2025 hebben wij u de door u gevraagde informatie per email toegezonden waarbij in sommige documenten bepaalde passages waren weggelakt (persoonsgegevens en gevoelige bedrijfsinformatie).

Op 14 augustus 2025 ontvingen wij van u het uitdrukkelijke verzoek om een Woo-besluit en een ingebrekestelling.

Om welke documenten het gaat leest u in de bijlage
Wij hebben gezocht naar de documenten die u openbaar wenst te maken. In de inventarisatielijst die wij als bijlage bijvoegen ziet u welke documenten wij hebben gevonden. Ook staat er vermeld of bepaalde informatie weggelakt is. Wij vermelden daarbij ook de wettelijke reden waarom wij de informatie moeten weglakken.

Besluit
Wij besluiten uw verzoek in te willigen. Hieronder volgt een toelichting.

Gedeeltelijk openbaar
De documenten met nummers 8 t/m 20 maken wij gedeeltelijk openbaar. De gehanteerde weigeringsgronden voor de geanonimiseerde delen zijn opgenomen in de inventarisatielijst.

Motivering weigeringsgronden
In de documenten 8 t/m 20 zijn de persoonsgegevens weggelakt.
Daarnaast hebben wij in deze documenten informatie weggelakt die betrekking heeft op mogelijke kwetsbaarheden in ons geautomatiseerde systeem en maatregelen om te voorkomen dat er van deze kwetsbaarheden gebruik kan worden gemaakt -door o.a. onbevoegden- waardoor er schade kan ontstaan -in de meest brede zin van het woord- bij onze organisatie en/of klanten die van de dienstverlening van onze organisatie afhankelijk zijn. Daarbij denken wij in het bijzonder aan hackers die deze informatie kunnen misbruiken.

Heeft u nog vragen?
Als u vragen heeft over deze brief, kunt u contact opnemen met de heer Walhof via het e-mailadres: h.walhof@stadsbankoostnederland.nl

Hoogachtend,

Stadsbank Oost Nederland,

G.W. Pol
Directeur Stadsbank Oost Nederland

Stadsbank
Oost Nederland

Bent u het niet eens met dit besluit?
Wij nemen deze beslissing volgens bepaalde wetten en regels, namelijk:
- Wet open overheid;
- Algemene wet bestuursrecht.

U kunt bezwaar maken binnen 6 weken na datum van deze brief
Na deze datum nemen we uw bezwaarschrift in de meeste gevallen niet meer in behandeling.

Ook als u bezwaar maakt blijft de inhoud van deze brief gelden

U kunt uw bezwaarschrift indienen bij de directie van de Stadsbank.

Digitaal:
E-mail:
wooverzoek@stadsbankoostnederland.nl

Brief per post:
Directeur Stadsbank Oost Nederland
Postbus 1393
7500 BJ Enschede

In uw bezwaarschrift moet in ieder geval het volgende staan:
1. uw naam, adres, telefoonnummer (en e-mailadres*);
2. het zaaknummer/kenmerk;
3. de datum waarop u de brief schrijft*;
4. waar u het niet mee eens bent;
5. waarom u het er niet mee eens bent;
6. uw handtekening*.

*Vermelden indien u het bezwaarschrift op papier aanlevert

Stadsbank
Oost Nederland

Inventarisatielijst bij Woo besluit (WOO verzoeken - 25-00001)

nr	Document	Beoordeling gevonden document	Uitzondering
1	Procedure melden van incidenten van 12-03-2018	Wordt openbaar gemaakt	
2	DB Voorstel informatiebeveiligingsbeleid van 12-04-2018	Wordt openbaar gemaakt	
3	Informatiebeveiligingsbeleid SON (versie 2018)	Wordt openbaar gemaakt	
4	procedure Configuratiebeheer van 2018	Wordt openbaar gemaakt	
5	DB-voorstel VVT van 05-07-2018	Wordt openbaar gemaakt	
6	De AVG en het inkoopproces 2018	Wordt openbaar gemaakt	
7	Algemene inkoopvoorwaarden 2018	Openbaar https://stadsbankoostnederland.nl/wp-content/uploads/2018/11/Algemene-inkoopvoorwaarden.pdf	
8	GIBIT-uitgave juni 2017	Wordt openbaar gemaakt	
9	Procedure Hardening van 12-03-2018	Wordt deels openbaar gemaakt	Art 5.1 lid 2 onder e en h WOO
10	Procedure Wijzigingsbeheer van 12-03-2018	Wordt deels openbaar gemaakt	Art 5.1 lid 2 onder e en h WOO
11	Wachtwoordbeleid Stadsbank Oost Nederland van 12-03-2018	Wordt deels openbaar gemaakt	Art 5.1 lid 2 onder e en h WOO
12	Verklaring van toepasselijkheid van 13-06-2018	Wordt deels openbaar gemaakt	Art 5.1 lid 2 onder e WOO
13	verslag Privacy Impact Assessment Beschermingsbewind	Wordt deels openbaar gemaakt	Art 5.1 lid 2 onder e en h WOO
14	Verklaring van toepasselijkheid 2019 van 03-05-2019	Wordt deels openbaar gemaakt	Art 5.1 lid 2 onder e WOO
15	Verslag DPIA Fundaments van januari 2020	Wordt deels openbaar gemaakt	Art 5.1 lid 2 onder e en h WOO
16	Calamiteitenplan Stadsbank Oost Nederland van 28-02-2023	Wordt deels openbaar gemaakt	Art 5.1 lid 2 onder e en h WOO

17	DPIA 2020 van 17-12-2020	Wordt deels openbaar gemaakt	Art 5.1 lid 2 onder e WOO
18	Verslag DPIA DATA B van januari 2024	Wordt deels openbaar gemaakt	Art 5.1 lid 2 onder e en h WOO
19	Handleiding mailbeveiliging	Wordt deels openbaar gemaakt	Art 5.1 lid 2 onder e WOO
20	DPIA 2024 van 22-01-2024	Wordt deels openbaar gemaakt	Art 5.1 lid 2 onder e WOO