HANDREIKING INFORMATIEBEHEER X:

GEMEENTELIJKE KWALITEITSNORMEN VOOR INKOOPVOORWAARDEN

Beleidsnotitie

Gemeente Almere

INHOUD

Inleiding 3

Gemeentelijke kwaliteitsnormen 4

Beveiligen 4

Beschermen 5

Beheren 6

Versie en status	0.9 Gebaseerd op eerdere handreiking E-HRM project en GIBIT
Datum	**21 augustus 2017**
Opdrachtgever	**Gemeente Almere**
Team/taakveld	**CIO Office**
Auteur(s)	**Frans Smit**
Versiegeschiedenis	**0.9 Gebaseerd op eerdere handreiking E-HRM project en GIBIT**

INLEIDING

Deze handreiking geeft invulling aan de Gemeentelijke Kwaliteitsnormen ten aanzien van informatieveiligheid, informatiebeheer en privacybescherming zoals bedoeld in de Gemeentelijke Inkoopvoorwaarden bij IT (GIBIT), die in opdracht van de VNG zijn ontwikkeld zijn door KING. Voor deze handreiking is gebruik gemaakt van de meest actueel beschikbare versie in drukvorm uit november 2016.

De handreiking is gebaseerd op een eerder uitgebracht advies van het CIO Office aan het project E-HRM in 2016. Uiteraard is de handreiking verder geactualiseerd.

De doelgroepen van de notitie zijn:

- De afdeling Inkoop van SBV;
- Het Team Contract- en Leveranciersmanagement van het CIO Office;
- Projectleiders van IV-projecten, voornamelijk werkzaam bij ICTAR;
- Proceseigenaren waarvan het proces, en daarmee dus ook de informatieverwerking, geheel en gedeeltelijk wordt uitbesteed aan derden;
- De afdeling Juridische Zaken;
- Het Tactisch Informatiebeheer Overleg (TIO).

De handreiking is zo praktisch mogelijk opgezet. Hij bevat per onderdeel van het Information Governance Framework: beschermen, beveiligen en beheren, een zo compact en zo helder mogelijk gestelde verzameling eisen.

GEMEENTELIJKE KWALITEITSNORMEN

BEVEILIGEN

Id	Omschrijving
1	De leverancier zal indien hij (pogingen tot) ongeautoriseerde toegang tot de systeemomgeving signaleert, alle noodzakelijke maatregelen nemen teneinde de eventuele schade tot een minimum te beperken en herhaling te voorkomen. De (poging tot) ongeautoriseerde toegang alsmede alle getroffen maatregelen zullen aan de gemeente worden gerapporteerd.
2	De leverancier garandeert dat ongeautoriseerde personen geen toegang hebben tot de gegevens van de gemeente, ook niet na beëindiging van de overeenkomst.
3	De leverancier garandeert dat data maandelijks, in een vooraf gedefinieerd formaat door de Gemeente Almere, worden geborgd bij een derde partij als zijn een Escrow-leverancier
4	De leverancier garandeert dat ongeautoriseerde personen geen toegang hebben tot gegevens of gegevensdragers (zoals harde schijven en back-upmedia) die tussentijds of na beëindiging van de overeenkomst worden verwijderd c.q. worden vervangen.
5	Voor gebruikers die vanuit het LAN inloggen op het systeem kunnen bij voorkeur via single sign on of via username/wachtwoord combinatie inloggen.
6	Bij datacommunicatie voor bestandsuitwisseling en voor de user interface wordt gebruik gemaakt van SSL versie 3 (Secure Sockets Layer) en cliënt- en servercertificaat technologie. User → Saas SSLv3 en enkelvoudig geldig certificaat. LAN ←→ Saas: Tweezijdig authenticatie middels certificaten.
7	De medewerker van de leverancier heeft in het systeem alleen toegang tot de aan hem geautoriseerde functies en gegevens.
8	Er is een totaaloverzicht beschikbaar van alle autorisaties van zowel de leverancier als de gemeente.
9	IT-voorzieningen en apparatuur bij de leverancier zijn fysiek beschermd tegen toegang door onbevoegden en tegen schade en storingen. De geboden bescherming is in overeenstemming met de vastgestelde risico's
10	Systeemsoftware die bij de leverancier in gebruik is, wordt up-to-date gehouden.
11	Situaties waarin meer dan normale kwetsbaarheden of risico's aanwezig worden onmiddellijk gemeld aan en besproken met de gemeente.
12	De gemeente laat door een door hen gekozen partij periodieke audits uitvoeren op de hierboven genoemde onderdelen.
13	De leverancier verleent medewerking aan het uitoefenen van controle door of namens de gemeente op bewaring en gebruik van gegevens, en naleving van procedures.

BESCHERMEN

Id	Omschrijving
14	De gemeente sluit met de leverancier een schriftelijke overeenkomst met betrekking tot de bescherming en de verwerking van persoonsgegevens cf. art 14 WBP. Daarbij wordt het model bewerkersovereenkomst van de gemeente gehanteerd.
15	De leverancier mag de door de gemeente verzamelde persoonsgegevens slechts in uitdrukkelijke opdracht van de gemeente verwerken. Persoonsgegevens mogen bovendien alleen worden verwerkt voor zover dat noodzakelijk is om de clouddiensten te leveren. De leverancier mag persoonsgegevens dus niet voor eigen doeleinden gebruiken
16	De leverancier mag bij het verwerken van de persoonsgegevens alleen groepsmaatschappijen en onderaannemers inschakelen met wie hij een schriftelijke overeenkomst heeft gesloten waarin geheimhoudings- en beveiligingsverplichtingen zijn opgenomen conform de berwerksovereenkomst.
17	De leverancier is verplicht de persoonsgegevens adequaat te beveiligen. De leverancier maakt expliciet welke beveiligingsmaatregelen met betrekking tot de door de gemeente verzamelde persoonsgegevens worden genomen. Bij de beveiligingsmaatregelen moet worden gedacht aan de eisen die hierboven onder Informayieveiligheid zijn omschreven. Tevens moet een actuele en volledige beschrijving van het gehanteerde beveiligingsbeleid beschikbaar zijn voor de gemeente.
18	De leverancier moet de gemeente in staat stellen om erop toe te zien dat hij zijn verplichting tot adequate beveiliging nakomt. Een bezwaar van de leverancier tegen een door de gemeente uit te voeren audit is niet acceptabel
19	Met de Privacy Information Officer moet een procedure worden afgesproken worden inzake rechtmatige inzageverzoeken van bevoegde autoriteiten.
20	De leverancier mag de persoonsgegevens niet langer bewaren dan noodzakelijk om de clouddiensten aan de gemeente te leveren. De leverancier moet garanderen en aantonen dat de gegevens na beëindiging van de overeenkomst worden vernietigd
21	De leverancier mag de persoonsgegevens alleen verwerken in de Europese Unie, in de Europese Economische Ruimte of in een land met passend beschermingsniveau. De data moeten encrypted worden opgeslagen waarbij de private key enkel in handen is van de gemeente of van een door de gemeente aangewezen gedelegeerde partij
22	De leverancier moet meewerken aan rechtmatige verzoeken van betrokkenen om inzage en correctie van hun persoonsgegevens conform afspraken met de Privacy Information Officer.
23	De leverancier neemt afdoende maatregelen inzake de Meldplicht Datalekken (art 34 WBP) conform de beleidsregels van Autoriteit Persoonsgegevens en de voorschriften van de Privacy Information Officer

BEHEREN

Id	Omschrijving
24	Het informatiebeheer moet gedocumenteerd zijn op de wijze zoals omschreven in artikel 4 van het Besluit Informatiebeheer Almere en nader uitgewerkt in de Handreiking Information Governance Framework van de gemeente. De documentatie moet actueel en volledig zijn, en beschikbaar voor de gemeente.
25	De leverancier moet tijdige en volledige medewerking verlenen aan het toezicht op het informatiebeheer door de gemeentelijke Informatiebeheer Officer, Records Management Officer en/of Archieftoezichthouder of andere daartoe bevoegde partijen.
26	De leverancier dient aantoonbaar de authenticiteit, de betrouwbaarheid, de integriteit en de bruikbaarheid van de beheerde informatie te waarborgen. Daartoe moeten de vorm, de structuur, de inhoud en het gedrag van archiefbescheiden behouden blijven.
27	De leverancier dient aantoonbaar de door de gemeente aangegeven bewaartermijnen te handhaven en verwijderingen pas na toestemming en conform de voorwaarden van de gemeente uit te voeren.
28	De leverancier dient archiefbescheiden die ontvangen of opgemaakt worden, op te nemen en te registreren conform afspraken met de gemeente
29	De leverancier dient de archiefbescheiden dusdanig te ordenen en te classificeren dat te allen tijde duidelijk is van welk bedrijfsproces zij de neerslag zijn
30	De leverancier dient aantoonbaar de archiefbescheiden te bewaren en te beveiligen conform de eisen van de gemeente
31	De leverancier moet te allen tijde de toegankelijkheid van de archiefbescheiden waarborgen voor medewerkers die toegang mogen hebben tot die bescheiden en tevens voor koppelingen met andere informatiesystemen.
32	De leverancier moet bij beëindiging van de overeenkomst aantoonbaar alle archiefbescheiden, en bijbehorende metadata, overdragen aan de gemeente conform tevoren afgesproken procedures en bestandsformaten. De leverancier verwijdert daarna aantoonbaar alle archiefbescheiden en metadata uit de beheeromgeving.
33	De leverancier moet archiefbescheiden kunnen migreren naar de archiefsystemen van de gemeente conform afspraken met de gemeente.
34	De leverancier moet de authenticiteit en de betrouwbaarheid actief en aantoonbaar beschermen door beveiligingsmaatregelen, controles en preservering