

Bijlage 8 IB-inkoopeisen

Inleiding

Alle onderstaande eisen komen voort uit o.a. het Kadaster Informatiebeveiligingsbeleid en de daar aan gerelateerde stukken. Dit is van toepassing op alle overeenkomsten die met het Kadaster worden gesloten. Dit beleidsstuk is aan verandering onderhevig net zoals de risico's die het Kadaster hiermee tot acceptabel niveau wil brengen. We verwijzen in dit document zoveel mogelijk naar zaken zoals best-practices vanuit de markt of overheid maar geven op sommige plekken concrete invulling aan specifieke eisen zoals die op dit moment zijn vastgesteld. Bij wijziging in het bovenliggende informatiebeveiligingsbeleid zullen de in dit document gestelde eisen dus tevens worden aangepast.

Data

1. Het Kadaster blijft te allen tijde eigenaar van haar data. De leverancier mag de data niet gebruiken voor andere doeleinden dan de afgesproken dienstverlening.
2. De leverancier biedt de mogelijkheid voor het Kadaster om bewaartermijnen van Kadaster data conform de Kadaster selectielijst in te richten. De leverancier zorgt ervoor dat de data na het verstrijken van de bewaartermijn op een veilige manier wordt verwijderd.
3. De leverancier draagt, na beëindiging van de te sluiten overeenkomst, de data van het Kadaster in een algemeen geaccepteerd bestandsformaat over en vernietigt de data van haar eigen systemen. De leverancier levert een bewijs van overdracht en vernietiging aan het Kadaster.
4. Datadragers met data van het Kadaster worden na beëindiging van gebruik of bij een defect aantoonbaar, middels een bewijs van een derde partij of eigen vernietigingsprocedure, ontoegankelijk gemaakt. De leverancier is verantwoordelijk voor het voorkomen van datalekken of ongeautoriseerde toegang tot de datadragers.
5. De locatie van de verwerking van data (daaronder begrepen maar niet beperkt tot: data in rust, productie, back-ups, etc.) vindt plaats binnen de Europese Economische Ruimte waar minimaal Europees recht van toepassing is. Voor zover (sub)verwerking plaatsvindt buiten de EER is dat alleen toegestaan op grond van door een bevoegde toezichthoudende autoriteit goedgekeurde bindende bedrijfsvoorschriften zoals is bedoeld en voor zover die voldoen aan alle eisen zoals genoemd in artikel 47 Algemene Verordening Gegevensbescherming. De leverancier informeert het Kadaster over de locaties waar de data wordt verwerkt en houdt het Kadaster op de hoogte van eventuele wijzigingen.
6. Alle fysieke & virtuele apparaten, systemen, softwareplatformen en applicaties die onderdeel zijn van de dienstverlening aan het Kadaster zijn uiterlijk vanaf ingebruikname geïdentificeerd en geregistreerd met vereiste (meta)gegevens in de Kadaster CMDB (thans ServiceNow), conform het CSDM-data-model.

Detectie, Response en Logging

1. Significante gebeurtenissen met betrekking tot de dienstverlening aan het Kadaster kunnen worden geïdentificeerd en worden geregistreerd bij de Managed Security Service (MSS).
2. De MSS, CERT-Retainer en SOC van het Kadaster kunnen te allen tijde toegang krijgen tot relevante (security) configuraties en audit logs van alle in de Kadaster CMDB opgenomen CI's t.b.v. triage, analyse, forensisch onderzoek en/of threat hunting.
3. Bij (vermoedelijke) securityincidenten dienen relevante logs conform de BIO termijnen (huidig minimaal 3 jaar) bewaard te worden of beschikbaar te worden gesteld aan de MSS van het Kadaster ter bewaring.

4. De leverancier werkt mee aan de implementatie en mogelijk deels geautomatiseerd toepassen van het Kadaster SOC/MSS stekkermandaat; om bepaalde onderdelen (tijdelijk) te isoleren en/of uit te schakelen, om de schade van een security incident te helpen beperken.
5. Alle vormen van logs dienen minimaal 6 maanden te worden bewaard om forensisch onderzoek mogelijk te maken in het geval (security)incidenten.
6. Inhoud en bescherming van logs voldoet aan de eisen van de BIO en het Kadaster Informatiebeveiligingsbeleid.
7. De leverancier heeft aantoonbaar maatregelen genomen tegen cyberrisico's op basis van een risico-inschatting die gedeeld is met het Kadaster.
8. Het Kadaster heeft het recht om securitytesten (zoals pentesten, red-teaming, ethical hacking) uit te (laten) voeren op de door de leverancier geleverde diensten. Een leverancier kan ervoor kiezen om securitytesten zelf uit te laten voeren indien deze voldoet aan de door het Kadaster gestelde scope, reikwijdte, frequentie en kwaliteit. Alle daaruit voortvloeiende relevante bevindingen en benodigde maatregelen worden gerapporteerd aan het Kadaster met, indien van toepassing, een plan van aanpak voor de implementatie.

Continuïteit

1. De leverancier voert wijzigingen gecontroleerd en beheerst door, zonder daarbij afbreuk te doen aan de continuïteit van de geboden dienstverlening. Hiervoor maakt de leverancier gebruik van een representatieve test- en/of acceptatie-omgeving.
2. Kritische kwetsbaarheden (met CVSS-score 9.0 en hoger) worden zo snel mogelijk gemitigeerd, securitypatches hiervoor worden binnen een week geïnstalleerd. Dit gebeurt op basis van een risicoanalyse.

Categorie	CVSS Score	Mitigatie	Patch
Kritiek	9.0-10.0	Direct	5 dagen
Hoog	7.0-8.9	Direct	14 dagen
Midden	4.0-6.9	7 dagen	30 dagen
Laag	0.1-3.9	14 dagen	60 dagen

- (a) Bij in-house ontwikkeling moet de leverancier zo spoedig mogelijk en binnen 1 dag belangrijke patches kunnen aanleveren.
 - (b) Voor overige termijnen verwijzen we naar de Standaard Patchmanagement.
3. De leverancier heeft continuïteitsplannen voor systemen die de dienstverlening aan het Kadaster betreffen, die jaarlijks worden getest op functie en werking, over de test wordt gerapporteerd aan het Kadaster. In de continuïteitsplannen wordt minimaal aandacht besteed aan:
 - (a) Identificatie van essentiële procedures voor bedrijfscontinuïteit.
 - (b) Er is een actueel en periodiek getest Disaster recovery plan aanwezig
 - (c) Wie het plan mag activeren en wanneer, maar ook wanneer weer gecontroleerd teruggaan wordt.
 - (d) Veilig te stellen informatie (aanvaardbaarheid van verlies van informatie).
 - (e) Prioriteiten en volgorde van herstel en reconstructie.
 - (f) Documentatie van systemen en processen.
 - (g) Kennis en kundigheid van personeel om de processen weer op te starten.
4. De leverancier heeft een back-up beleid vastgesteld en geïmplementeerd waarin de RTO en RPO en eisen omtrent bescherming zijn gedefinieerd. Dit voldoet aan de eisen vanuit de BIO en volgt best-practices (<https://www.ncsc.nl/onderwerpen/back-ups>). Het Kadaster stelt de volgende verplichtingen met betrekking tot back-ups en Disaster Recovery (DR);

- (a) De DR-back-up is immutable opgeslagen met een retentietijd van minimaal 2 weken. Onder immutable wordt verstaan Write-Once-Read-Many opslag van de back-up data.
 - (b) De DR-back-up is netwerk-gescheiden van de productie en van de standaard back-up omgeving, bij voorkeur met airgap. Met airgap wordt bedoeld, dat de DR-back-up alleen tijdens het back-up proces bereikbaar is vanuit de back-up omgeving.
 - (c) Wanneer de DR-back-up op een online medium opgeslagen wordt, moeten voor de toegang tot de DR-back-up aparte credentials gebruikt worden, gescheiden van credentials voor gebruik en beheer van het productiesysteem.
 - (d) Alle back-ups moeten versleuteld opgeslagen worden, ook de DR-back-up.
 - (e) De RTO is maximaal 16 werkuren¹ of sneller indien geëist vanuit de BIA
 - (f) De RPO is maximaal 28 uur, of sneller indien geëist vanuit de BIA
5. Klantenomgevingen van leverancier zijn logisch gescheiden en kunnen elkaar onderling niet beïnvloeden als gevolg van verstoringen in de klantenomgeving.

Personeel

1. Medewerkers van de leveranciers die toegang hebben tot data van het Kadaster hebben een geheimhoudingsplicht en zijn gescreend voor hun functie (VOG met minimaal functieaspecten 11, 12, 13 of minimaal gelijkwaardig).
 - (a) In het geval dat er toegang is tot data van een classificatie boven BBN2 en/of vertrouwelijk niveau stelt het Kadaster mogelijk aanvullende eisen aan deze screening op basis van een risicoafweging.
2. De leverancier heeft zelf gedragsregels voor acceptabel gebruik van eigen bedrijfsmiddelen en alle medewerkers worden hier minimaal jaarlijks aantoonbaar op gewezen.
3. De leverancier stelt zijn medewerkers minimaal jaarlijks op de hoogte van de procedure waarop zij beveiligingsincidenten en datalekken moeten aanmelden.
4. Binnen de organisatie van de leverancier zijn de verantwoordelijkheden, taken en bevoegdheden voor het risicobeheer, Informatiebeveiliging en compliance vastgesteld en belegd.
 - (a) Controle op rechten gebeurt minimaal jaarlijks
 - (b) Controle op beheerrechten gebeurt minimaal halfjaarlijks
5. Medewerkers van de leverancier hebben enkel toegang tot Kadaster data op need-to-know basis. De lijst met medewerkers van de leverancier met toegang tot Kadaster data wordt minimaal ieder kwartaal aantoonbaar beoordeeld door de leverancier en de leverancier koppelt de resultaten terug aan het Kadaster. De leverancier zorgt ervoor dat de medewerkers die toegang hebben tot Kadaster data voldoende zijn getraind en geïnstrueerd over de geldende regels en procedures.

Ontwikkeling en life-cycle

1. De gangbare principes rondom Security-by-design (zoals vastgelegd in 'Beleids- en beheersingsrichtlijnen voor de ontwikkeling van veilige software' van het NCSC op <https://www.ncsc.nl>) zijn uitgangspunt voor de ontwikkeling van software en systemen
2. Voor acceptatietesten van software worden gestructureerde testmethodieken gebruikt. De testen worden bij voorkeur geautomatiseerd uitgevoerd.
3. Ten behoeve van de afgenomen dienstverlening dient de leverancier gebruik te maken van een gescheiden ontwikkel-, test-, acceptatie- en/of productieomgeving. Deze omgevingen zijn strikt gescheiden.

¹ In het geval van een calamiteit uiterlijk een week voor onderdelen uit een bedrijfskritisch onderdelen.

4. Bij het ontwikkelen en testen wordt bij voorkeur gebruik gemaakt van synthetische gegevens. Gebruik van data van het Kadaster voor ontwikkel/testen is enkel toegestaan na expliciete toestemming.
5. De leverancier heeft aantoonbaar effectieve patch- & lifecycle- managementprocessen t.a.v. alle fysieke & virtuele apparaten, systemen, softwareplatformen en applicaties die onderdeel zijn van de dienstverlening aan het kadaster. Waarbij alle onderdelen onder actieve contractuele (security) support vallen van de leveranciers en zo binnen gestelde SLA tijden van de security patches worden voorzien.

Digitale toegang

1. De volgende eisen zijn van toepassing voor zover Kadaster gebruikers op IT-componenten kunnen inloggen die onderdeel zijn van de geleverde dienst, of voor zover deze IT-componenten toegang geven tot Kadaster data en/of functionaliteit. Van deze eisen mag enkel worden afgeweken na een risicoafweging door Kadaster conform de procedure Uitzondering op beleid.
 - (a) De leverancier maakt het mogelijk dat de geleverde IT-componenten worden aangesloten op de Kadastervoorziening(en) voor authenticatie, gebaseerd op open standaarden (lijsten 'verplicht' en 'aanbevolen' van Forum voor Standaardisatie).
 - (b) De leverancier maakt het mogelijk dat de geleverde IT-componenten worden aangesloten op de Kadastervoorziening voor autorisatiebeheer, gebaseerd op open standaarden (lijsten 'verplicht' en 'aanbevolen' van Forum voor Standaardisatie). De wijze van aansluiten dient zodanig te worden vormgegeven dat het toekennen, wijzigen of intrekken van toegangsrechten automatisch plaatsvindt.
 - (c) De leverancier maakt het mogelijk dat de geleverde IT-componenten worden aangesloten op de Kadastervoorziening voor beveiligen van kritieke toegang, gebaseerd op open standaarden (lijsten 'verplicht' en 'aanbevolen' van Forum voor Standaardisatie). De wijze van aansluiten dient zodanig te worden vormgegeven dat de inloggegevens door de Kadaster voorziening automatisch kunnen worden gewijzigd.
2. Voor zover medewerkers van de leverancier toegang nodig hebben tot IT-componenten van Kadaster die de leverancier zelf niet levert, worden de autorisaties beheerd middels het leveranciersportaal dat onderdeel is van de Kadastervoorziening voor autorisatiebeheer. Van deze eisen mag enkel worden afgeweken na een risicoafweging door Kadaster conform de procedure Uitzondering op beleid.

Cryptografie

1. De leverancier maakt het mogelijk voor Kadaster om eigen beheer over haar certificaten te voeren op de geleverde omgeving. Dit is een eis op (sub)domeinen van het Kadaster en een sterke voorkeur bij overige domeinen (zoals die van een leverancier zelf).
2. Niet openbare gegevens inclusief persoonsgegevens worden altijd versleuteld in transport (over niet Kadaster netwerken) en bij opslag. Versleuteling in transport en opslag voldoet aan de hedendaagse geaccepteerde standaarden voor versleuteling in opslag (waaronder minimaal de richtlijnen van NCSC).

Standaarden (waar van toepassing)

3. API's die de oplossing bieden om het systeem te integreren met Kadaster systemen gebruiken protocollen die zijn aanbevolen door Forum Standaardisatie (<https://www.forumstandaardisatie.nl/open-standaarden/aanbevolen>).

4. De oplossing voldoet aan de verplichte standaarden van het Forum Standaardisatie (<https://www.forumstandaardisatie.nl/open-standaarden/verplicht>).
5. De leverancier versleutelt bij communicatie met het Kadaster alle berichten en bestandsuitwisselingsmogelijkheden.
6. Indien cookies nodig zijn, dienen deze versleuteld te worden.

Rapportage en Verantwoording

1. Beveiligingsincidenten en datalekken die impact hebben op de aan het Kadaster aangeboden dienstverlening en/of data worden zo snel mogelijk (maar uiterlijk binnen 24 uur) gemeld door de leverancier aan het Kadaster. Het meldpunt is de ServiceDesk. Telefoon: +31 (0)88-183 21 00, KSD@kadaster.nl.
2. Om de effectiviteit van de maatregelen, compliance aan het beleid en voldoen aan wet- en regelgeving te kunnen waarborgen, heeft het Kadaster de mogelijkheid om dit te verifiëren middels een formele audit. De leverancier kan dit ook zelf aantonen middels een onafhankelijke audit door een gecertificeerd auditor met inachtneming van de juiste scope en reikwijdte. Het niet voldoen aan de mogelijkheid om een audit te laten uitvoeren dan wel het niet opleveren van de juiste assurance verklaringen kan leiden tot het voortijdig beëindigen van de overeenkomst.
3. Het algemene niveau van de informatiebeveiliging blijkt uit één van het volgende:
 - (a) Periodieke externe controles zoals audits, pentesten of TPM's (bijv. ISO27001 inclusief Verklaring van Toepasselijkheid, ISAE3000 (ookwel SOC T2));
 - (b) Een Assurance rapport van een auditor die is aangesloten bij NOREA én in het bezit is van de RE certificering;

De eventuele kosten voor het aantonen van de toereikendheid en/of het opvolgen van eventuele adviezen zijn voor de leverancier. De adviezen dienen te worden uitgewerkt in een plan van aanpak en te worden overlegd met het Kadaster. Na akkoord van het Kadaster, voor het uitvoeren van het plan van aanpak, dienen de maatregelen binnen 2 maanden geïmplementeerd te zijn tenzij anders overeengekomen. Indien de leverancier niet kan of niet wenst te voldoen aan de aanbevelingen en adviezen in het auditrapport, heeft het Kadaster de mogelijkheid tot opzeggen van de te sluiten overeenkomst.

4. De leverancier rapporteert minimaal elk kwartaal schriftelijk over informatiebeveiligingsrisico's (inclusief kans en impact, genomen beheersmaatregelen en eventuele restrisico's) aan het Kadaster.
5. De leverancier voert jaarlijkse een BIO self-assessment uit, waarbij hij aantoont dat de informatiebeveiliging voldoet aan het gestelde normenkader. In het kader van het Pas toe of Leg uit principe dient de leverancier afwijking van het genoemde normenkader toe te lichten.
6. De leverancier heeft een vastgestelde procedure voor beveiligingsincidenten (CVD) en datalekken, waarin de taken en verantwoordelijkheden staan beschreven. De beschreven taken en bevoegdheden zijn belegd in de organisatie.
7. De leverancier is verantwoordelijk voor de beveiliging van de eigen organisatie en dienstverlening conform de door het Kadaster te stellen eisen, aangevuld met het volgen van branche-richtlijnen en standaarden.
8. De leverancier is verantwoordelijk voor het leveren van veilige diensten aan het Kadaster, en regelt daartoe een adequaat systeem in (processen, medewerkers, tooling, monitoring) voor de eigen dienstverlening.