

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 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. 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.
5. De leverancier heeft aantoonbaar maatregelen genomen tegen cyberrisico's op basis van een risico-inschatting.

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 melden.
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.

Cryptografie

1. 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).

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 (ook wel SOC T2));
 - b. Een Assurance rapport van een auditor die is aangesloten bij NOREA én in het bezit is van de RE certificering;