KNOWLEDGE BY DATA

Kwetsbaarhedenbeleid

Coordinated Vulnerability Disclosure — Knowledge by Data B.V.

Hoe u een kwetsbaarheid meldt, wat u van ons mag verwachten en hoe wij onze producten ondersteunen

OPENBAAR

Uitgever: Knowledge by Data — Professionele analyse-instrumenten voor de publieke sector
Datum: 9 september 2026
Doelgroep: Afnemers, beveiligingsonderzoekers, toezichthouders
Status: Definitief

Documentinformatie

Veld	Waarde
Document	Kwetsbaarhedenbeleid (Coordinated Vulnerability Disclosure)
Organisatie	Knowledge by Data B.V., Mient 24 B, 1811 NC Alkmaar, KvK 99430169
Grondslag	Cyber Resilience Act (Verordening (EU) 2024/2847), bijlage I deel II; Leidraad Coordinated Vulnerability Disclosure van het NCSC
Meldadres	security@knowledgebydata.nl · https://www.knowledgebydata.nl/.well-known/security.txt
Datum	9 september 2026
Versie	1.0
Classificatie	Openbaar
Status	Definitief — van kracht

Inhoudsopgave

1. Waarom dit beleid

Knowledge by Data B.V. (“KbD”) levert analysesoftware aan gemeenten en andere overheidsorganisaties. Die software verwerkt gevoelige gegevens en draait bewust volledig lokaal, zonder verbinding naar buiten. Juist daarom vinden wij het belangrijk dat iedereen die een zwakte ontdekt — een afnemer, een beveiligingsonderzoeker, een toezichthouder — ons die veilig en eenvoudig kan melden, en weet wat er dan gebeurt.

Dit beleid beschrijft die afspraken. Het geeft uitvoering aan de eisen die de Europese Cyber Resilience Act aan fabrikanten van software stelt: een beleid voor gecoördineerde openbaarmaking, een contactpunt, beveiligingsupdates gedurende een vastgestelde ondersteuningsperiode en een softwarestuklijst per product.

2. Reikwijdte

Dit beleid geldt voor alle software die KbD in de handel brengt (de analyseapplicaties, de Readers en de KBD Analysis Suite) en voor de diensten waarmee wij die software leveren en ondersteunen.

Het geldt niet voor systemen van onze afnemers waarop de software is geïnstalleerd; meldingen daarover gaan naar de betreffende organisatie. Treft u in onze software een probleem aan dat de gegevens van een afnemer raakt, meld het dan aan ons; wij informeren de afnemer.

3. Een kwetsbaarheid melden

Meld een kwetsbaarheid vertrouwelijk via:

- E-mail: security@knowledgebydata.nl (dit adres wordt bewaakt; buiten kantooruren ten minste dagelijks).
- Alternatief: het algemene adres lpantenbrink@knowledgebydata.nl, onder vermelding van “kwetsbaarheid”.
- Machineleesbaar: https://www.knowledgebydata.nl/.well-known/security.txt (RFC 9116), ook op alle *.knowledgebydata.nl-diensten.

Vermeld in uw melding zo mogelijk: welk product of welke dienst en welke versie; wat u hebt aangetroffen en hoe het te reproduceren is; wat de mogelijke impact is; en hoe wij u kunnen bereiken. Screenshots en een stappenlijst helpen. Stuur ons geen gegevens van derden mee die u tijdens uw onderzoek bent tegengekomen.

Wilt u versleuteld mailen, vermeld dat dan in een eerste bericht; wij sturen u een sleutel.

4. Wat wij doen na uw melding

- Binnen 1 werkdag ontvangt u een ontvangstbevestiging.
- Binnen 5 werkdagen laten wij u weten of wij de melding als kwetsbaarheid erkennen en hoe ernstig wij haar inschatten.
- Wij houden u op de hoogte van de voortgang en overleggen met u over het moment van openbaarmaking.
- Een erkende kwetsbaarheid verhelpen wij in een nieuwe, ondertekende versie die via onze vaste uitrolketen bij alle afnemers terechtkomt. Streeftermijn: ernstige kwetsbaarheden binnen 30 dagen, overige binnen 90 dagen na erkenning.
- Blijkt een kwetsbaarheid actief te worden misbruikt, dan melden wij dat — los van uw melding — aan ENISA en het Nationaal Cyber Security Centrum, zoals de Cyber Resilience Act voorschrijft, en informeren wij onze afnemers direct.

5. Wat wij van u vragen

- Meld de kwetsbaarheid zo snel mogelijk en alleen aan ons, en deel haar niet met anderen totdat wij haar hebben verholpen en samen een moment van openbaarmaking hebben afgesproken.
- Ga niet verder dan nodig is om de kwetsbaarheid aan te tonen: geen gegevens kopiëren, wijzigen of verwijderen; geen toegang tot systemen of gegevens van afnemers; geen aanvallen die de beschikbaarheid raken; geen sociale manipulatie van medewerkers of afnemers.
- Maak geen gebruik van de kwetsbaarheid en installeer geen achterdeuren.
- Behandel gegevens die u onbedoeld bent tegengekomen als vertrouwelijk en verwijder ze zodra u ze niet meer nodig hebt.

6. Geen juridische stappen bij verantwoord handelen

Handelt u volgens dit beleid, dan onderneemt KbD geen juridische stappen tegen u en doet zij geen aangifte in verband met uw onderzoek. Wij beschouwen uw melding als een bijdrage aan de veiligheid van onze afnemers, niet als een aanval.

Dit beleid sluit aan bij de Leidraad Coordinated Vulnerability Disclosure van het NCSC. Het geeft geen vrijbrief voor handelen dat buiten de reikwijdte van hoofdstuk 5 valt.

7. Ondersteuningsperiode en beveiligingsupdates

Elke productlijn van KbD wordt ten minste vijf jaar vanaf de datum van dit beleid, en in elk geval ten minste vijf jaar vanaf het in de handel brengen van een nieuwe productlijn, ondersteund met beveiligingsupdates. Voor de huidige producten betekent dit: ondersteuning tot ten minste 2031-09-09.

Per versie geldt: een versie wordt ondersteund tot zes maanden na het verschijnen van haar opvolger. Wij raden afnemers aan altijd de meest recente versie te installeren; de portal toont per product de actuele versie.

Beveiligingsupdates worden kosteloos en zonder onnodig uitstel beschikbaar gesteld, los van functionele updates waar dat kan. Elke uitgeleverde versie is digitaal ondertekend (Windows: Authenticode met het EV-certificaat van Knowledge by Data B.V.), zodat de afnemer kan vaststellen dat een update werkelijk van KbD komt.

De ondersteuningsperiode per product staat ook in de softwarestuklijst van dat product (hoofdstuk 9).

8. Hoe updates u bereiken

KbD-software werkt bewust zonder verbinding naar buiten en werkt zichzelf dus niet automatisch bij. Nieuwe versies worden gepubliceerd op de portal en de downloadserver; afnemers ontvangen bij een beveiligingsupdate een bericht op het bij ons bekende contactadres. De Readers (voor het inzien van dossiers na afloop van een licentie) volgen dezelfde route.

Een update installeert u als een nieuwe versie over de bestaande heen; dossiers en instellingen blijven behouden. De installatiehandleiding per product beschrijft de stappen.

9. Softwarestuklijst (SBOM)

Voor elk product houdt KbD een softwarestuklijst bij in het CycloneDX-formaat: alle meegeleverde bibliotheken en programma’s met versie en controlesom, en de bouwafhankelijkheden. Afnemers ontvangen de SBOM van hun producten op verzoek via security@knowledgebydata.nl; toezichthouders krijgen inzage in het conformiteitsdossier.

10. Openbaarmaking en naamsvermelding

Na het verhelpen van een kwetsbaarheid publiceert KbD een korte beschrijving in de versiegeschiedenis van het product. Wilt u als melder genoemd worden, dan doen wij dat graag; wilt u dat niet, dan blijft u anoniem. Openbaarmaking gebeurt in overleg en niet voordat afnemers de gelegenheid hebben gehad de herstelde versie te installeren.

11. Contact

Knowledge by Data B.V. — Mient 24 B, 1811 NC Alkmaar — KvK 99430169 — www.knowledgebydata.nl

Beveiligingsmeldingen: security@knowledgebydata.nl. Overige vragen: lpantenbrink@knowledgebydata.nl.

Dit beleid wordt ten minste jaarlijks herzien. De actuele versie staat op https://www.knowledgebydata.nl/kwetsbaarhedenbeleid.html.