

Algemene informatie

Aanbesteding: Productie en Levering Druk en Printwerk inclusief DTP werkzaamheden
Aanbestedende Dienst: UWV
Referentie: CG.2026.1048

Toelichting:

Deze vraag is binnen gekomen nav de eerste ronde NvI en is relevant voor alle betrokken partijen.

Vraag en antwoord

Ref.nr. 176
Onderwerp: NvI 36 & 39

Vraag:

Eis 106 verlangt dat Opdrachtnemer een volledige SBOM onderhoudt "voor de geleverde software". Die SBOM moet bij iedere update en/of nieuwe versie worden geleverd, in een machinaal leesbaar CycloneDX- of SPDX-formaat. Artikel 12.2 lid 1 sub c BVO bevat een SBOM-plicht "conform de huidige standaard formaten of andere(n) gewenst door UWV". In de antwoorden op ref. 36 en 39 geeft UWV aan dat er nog geen beleid of richtlijn is voor de SBOM. Frequentie, formaat, inhoud en risicoprofiel zijn nog niet vastgesteld. In ref. 36 heeft UWV een jaarlijkse SBOM met ISO 27001-certificaat afgewezen, maar zonder aan te geven wat dan wél volstaat. De concrete vragen in ref. 39 over reikwijdte en alternatief bewijs zijn niet inhoudelijk beantwoord. Tegelijk legt eis 106 wel al een formaat en een leverfrequentie vast. Omdat alle PvE-eisen knock-outeisen zijn (zie ref. 40), weet een inschrijver nu niet waaraan hij zich onvoorwaardelijk verbindt.

Elders in de NvI heeft UWV voor SaaS-platforms van derden al proportionele oplossingen aanvaard:

- Volgens ref. 38 test het Cyber Security Centre van UWV in beginsel alleen het webportaal en de koppelingen. Voor bevindingen buiten de invloedssfeer van Opdrachtnemer worden in overleg realistische hersteltermijnen afgesproken.
- Volgens ref. 66 mag de SaaS-leverancier bedrijfsvertrouwelijke informatie rechtstreeks en onder geheimhouding aan UWV verstrekken. Een recent onafhankelijk pentestrapport, een ISO 27001-certificaat of een ISAE 3402-/SOC 2-rapport mag daarbij in de plaats komen van broncodefragmenten.
- Volgens ref. 156 sluit UWV de BVO alleen met de leverancier (verwerker) en niet met subverwerkers. Als ISO 27001-certificering ontbreekt, beoordeelt UWV of de getroffen maatregelen gelijkwaardig zijn.
- Volgens ref. 40 en 113 heeft UWV de impact van de Cyber Resilience Act nog niet vertaald naar beleid. Voor maatwerk zoals een specifiek ingerichte bestelportal is volgens UWV niet zonder meer duidelijk of, en zo ja welke, CRA-verplichtingen gelden. Verplichtingen worden niet getoetst vóór de datum waarop zij in werking treden. Sinds 11 september 2026 geldt wel de meldplicht voor fabrikanten bij actief misbruikte kwetsbaarheden en ernstige incidenten.

Een inschrijver die standaard SaaS-platforms van derden inzet, beschikt niet zelf over een volledige SBOM van die software. Hij kan niet garanderen dat hij die per release verstrekt zonder medewerking van de technologieleverancier. Ter vergelijking: in de aanbesteding Grafische Dienstverlening voor de Rijksoverheid (kenmerk 201865002.155.084) wordt informatie verwerkt tot het niveau Departementaal vertrouwelijk. Daar volstaat als bewijs een ISO 27001-certificaat met jaarlijkse geaccrediteerde audit.

Met het oog op artikel 1.10 Aanbestedingswet 2012 en de Gids Proportionaliteit verzoeken wij UWV om de SBOM-verplichting voor deze platforms in lijn te brengen met de benadering in ref. 38, 66 en 156.

Wij vragen UWV de volgende vragen afzonderlijk te beantwoorden:

4. Handhaving en toekomstig beleid: Als UWV de verplichting voor deze platforms handhaaft, wil UWV dan vóór de sluitingsdatum het volgende vastleggen: de scope, de inhoud, de levermomenten, de vertrouwelijkheidswaarborgen en de acceptatiecriteria? En wil UWV motiveren

waarom het alternatief onvoldoende is? Wij vragen UWV daarnaast te bevestigen dat beleid dat later wordt vastgesteld, ook beleid over de CRA, niet leidt tot aanvullende verplichtingen zonder voorafgaande afspraken over uitvoerbaarheid, planning en kosten. Dat zou aansluiten bij artikel 7.1 lid 2 en lid 8 BVO en bij het antwoord op ref. 40 onder c).

Antwoord:

dit antwoord geldt voor vragen 176 t/m 179:

Wij gaan mee in uw verzoek om de eis te versoepelen, omdat UWV bij nader inzien eveneens van mening is dat de eis inzake het aanleveren van een Software Bill of Materials (SBOM), gezien de aard van de dienstverlening, niet proportioneel is.

Programma van Eisen versie 1.1 wordt hierop aangepaste.

Fase:

Inschrijffase

Inschrijfronde:

Inschrijfronde 1

Vragenronde:

Vragenronde 2

Beantwoord op:

22 okt 2026

Percelen:

P1 Productie en Levering Druk en Printwerk inclusief DTP werkzaamheden