Toelatingsvoorwaarden Rechtwijzer

(i) Aanbieder

De aanbieder is transparant over wie hij is en wat zijn achtergronden zijn, aan welke organisatie hij is verbonden en wie er (nog meer) investeert in het product/dienst. Hierbij kan bijvoorbeeld worden gedacht aan:

- Het is transparant en controleerbaar wie er achter het product/dienst zit.
- (Indien van toepassing) Het is transparant en controleerbaar wie er (nog meer) in het product/dienst investeert, en wat de investeringsvoorwaarden zijn.
- De aanbieder kan aantonen dat hij een gevestigde reputatie heeft, bijvoorbeeld door zijn productaanbod, klantbereik, omzet, klantwaardering of andere vormen van reviews.

(ii) Kwaliteit dienst/product

De aanbieder onderbouwt de kwaliteit van zijn product/dienst. Hierbij kan bijvoorbeeld worden gedacht aan:

- Onderbouwde en waar mogelijk bewezen kwaliteit van het product/dienst en de methode die daaraan ten grondslag ligt, bijvoorbeeld blijkend uit wetenschappelijke publicaties, een evaluatie van een onafhankelijke, gezaghebbende deskundige/deskundig instituut en/of ondersteund door bewezen best practices.
- Een toelichting op de wijze waarop het product/dienst de zelf- en samenredzaamheid van gebruikers/partijen stimuleert en hoe het product/dienst kan bijdragen aan een oplossing (resultaatgerichtheid).
- Een toelichting op de wijze waarop de geboden informatie en advies wordt onderhouden (up-to-date en inhoudelijk juist) en de standaarden die voor de informatie en adviezen worden gehanteerd (bijvoorbeeld objectieve informatie).
- Een toelichting op de gebruiksvriendelijkheid, bijvoorbeeld uitgevoerde gebruikerstests of focusgroepen en het gebruik klare taal.
- Een toelichting op de design standaarden, zoals responsiveness met smartphones, tablets, grafische vormgeving, gebruik van audio en video-middelen, de wijze waarop de webrichtlijnen worden nageleefd.
- (Indien van toepassing) Een toelichting op de wijze waarop de onlinevoorziening is geïntegreerd met of verwijst naar persoonlijke dienstverlening.
- (Indien van toepassing) Een beschrijving van de kwaliteitseisen waaraan de dienstverlener(s) die voor de aanbieder werken, moet(en) voldoen, bijvoorbeeld voldoen aan de voor het rechtsgebied waarvoor de toelating wordt gevraagd, geldende inschrijfvoorwaarden van de Raad; als met niet-juristen wordt gewerkt, voldoen aan de beschreven en uitgewerkte kwaliteitseisen zoals gesteld door de betreffende beroepsgroep. Verder kan worden gedacht aan de beschrijving van de wijze waarop de kwaliteit van de dienstverlener(s) wordt onderhouden, zoals peer review of permanente deskundigheidsbevordering. Ook moet duidelijk blijken dat de dienstverleners in staat worden gesteld om te voldoen aan de gedragsregels en verordeningen van de eigen beroepsgroep. NB: Inherent aan innovatie is dienstverlening op een nieuwe wijze wordt uitgevoerd, waarin niet is voorzien in de geldende regels. In dat geval dient de aanbieder aan de hand van een advies, bijvoorbeeld van een in het tuchtrecht gespecialiseerde expert, te onderbouwen dat de dienstverlening niet in strijd is met de regels zoals gesteld door de beroepsorganisatie.

(iii) Dienstverlening

De aanbieder heeft zijn organisatie ingericht op het bieden van goede dienstverlening aan gebruikers van zijn product/dienst. Hierbij kan bijvoorbeeld worden gedacht aan:

- Een klantcontactcentrum.
- Het periodiek uitvoeren van klanttevredenheidsonderzoek waarvan de resultaten gedeeld worden met de Raad.

• Aanwezigheid van een klachtprocedure.
• Aanwezigheid van een privacyreglement dat er ook in voorziet dat er geen data worden verzameld voor commerciële doeleinden en dat er geen sprake is van 'clickbait'.
• (Indien van toepassing) Er zijn algemene voorwaarden.
• Er is een gebruikersovereenkomst tussen de aanbieder en de klant.
• Er zijn overeenkomst(en) van opdracht tussen de dienstverlener en de klant indien sprake is van dienstverlening.

(iv) Security

De aanbieder moet inzicht kunnen geven over hoe de informatiebeveiliging is ingericht.

Afhankelijke van het type en aantal persoonsgegevens dat door de aanbieder wordt verwerkt zal de Raad beoordelen of er voldoende beveiligingsmaatregelen zijn toegepast.

Aspecten die door de Raad kunnen worden meegenomen in de beoordeling van de aanvraag zijn:

- Certificeringen op gebied van informatiebeveiliging (bijv. ISO 27001)
- De beschikking over een up to date[1] informatiebeveiligingsbeleid.
- Applicaties moeten compliant zijn met de ICT Beveiligingsrichtlijnen voor webapplicaties van het Nederlands Cyber Security Center (NCSC)[2]
- Applicaties moeten compliant zijn aan de verplichte standaarden van het forum standaardisatie[3] zoals o.a.
    - Email (DKIM, DMARC, SPF en STARTTLS en DANE)
    - Internetverbinding via (DKIM, HTTPS en HSTS, IPv4 en IPv6, SAML, STARTTLS en DANE, TLS en WPA2 Enterprise)
    - Website vereisten (BWB, DNSSEC, DMARC, Digitoegankelijk, SPF, STARTTLS en DANE, HTTPS en HSTS)
    - De certificaten kunnen gewone SSL certificaten of EV SSL certificaten zijn waarbij de voorkeur uitgaat naar EV SSL certificaten.
- Indien door de rijksoverheid voorgeschreven, moet er gebruik gemaakt worden van PKI overheidscertificaten.
- Gegevens moeten encrypted worden opgeslagen.
- Met de leveranciers die gegevens bewerken moet een bewerkersovereenkomst worden afgesloten die onderdeel uitmaakt van het contract. Binnen de bewerkersovereenkomst is aandacht voor zowel de huidige wet Datalekken als de toekomstige verordening van de Europese Unie, Algemene Verordening Gegevensbescherming.
- Voor de authenticatie van gebruikers kan gebruik gemaakt worden van verschillende methoden;
- i. DigiD: Eisen zijn conform de voorschriften van Logius, inclusief jaarlijkse audit
- ii. Userid / Wachtwoord: Indien gebruik gemaakt wordt van userID en wachtwoord, moet het wachtwoord minimaal voldoen aan de eisen die gesteld worden door de Raad voor de toegang tot de werkplek (minimaal 12 tekens en complex van aard) en MFA). Aanvraag van het wachtwoord is via een bevestiging op het eigen emailadres.
- Inzage in de autorisatieprocedure van de gebruikers die werken binnen de applicaties.
- Inzage in de inrichting van logging en monitoring.

[1] Niet ouder dan 3 jaar.
[2] ICT-beveiligingsrichtlijnen voor webapplicaties | Publicatie | Nationaal Cyber Security Centrum (ncsc.nl)
[3] 'Pas toe leg uit' standaarden (verplicht) | Forum Standaardisatie

- Het periodiek uitvoeren of laten uitvoeren van audits/pentesten[4] op de applicatie en infrastructuur (op productieomgeving).
- Inzage in de procedure omtrent de ontwikkeling en testen van (nieuwe) applicaties.

De beveiligingseisen moeten worden toegelicht aan de hand van onderbouwende documentatie.

(v) Privacy

De aanbieder moet inzicht kunnen geven over hoe de privacy van de betrokkenen wordt gewaarborgd en of er wordt voldaan aan de verplichtingen die de privacy wet- en regelgeving stelt[5].

De Raad zal globaal beoordelen of de privacy van de betrokkenen voldoende beschermd wordt in de verwerking van hun persoonsgegevens. Aspecten die door de Raad kunnen worden meegenomen in de beoordeling van de aanvraag zijn:

- Een recente en actuele Data Protection Assessment (DPIA).
    - Op advies van de Autoriteit Persoonsgegevens is het aan te raden om periodiek een DPIA uit te voeren. Om die reden stellen wij als vereiste dat de DPIA maximaal 3 jaar oud mag zijn tenzij beargumenteerd weerlegd kan worden dat er vanaf vaststelling van de DPIA geen wijzigingen in de verwerking hebben plaatsgevonden.
    - De DPIA moet in ieder geval de volgende aspecten bevatten[6]:
        - Een systematische beschrijving van gegevensverwerking en de doeleinden van deze verwerking
        - De noodzaak en proportionaliteit van de verwerking
        - De privacy risico's van de betrokkenen
        - De maatregelen om de vastgestelde risico's te mitigeren en om aan te tonen dat voldaan wordt aan de AVG
- De genomen technische en organisatorische maatregelen om de persoonsgegevens te beveiligen.
- De privacyverklaring voor de betrokkenen.
- De locatie van de verwerking van persoonsgegevens. De persoonsgegevens moeten worden opgeslagen in een database en op een server die binnen de grenzen van de Europese Economische Ruimte ligt.
- Als andere partijen persoonsgegevens verwerken voor/namens de aanbieder moet er een verwerkersovereenkomst zijn afgesloten met deze partij.
- De toepassing van Privacy by Design en Privacy by Default op de verwerking van persoonsgegevens.
- Overige verplichtingen die de privacy wet- en regelgeving stelt en van toepassing zijn op de applicatie. Denk hierbij aan:
    - Rechtmatige grondslag;
    - De betrokkenen kunnen de rechten van betrokkenen uitoefenen
    - Verwerkingsregister is up to date
    - Proces voor datalekken is aanwezig
    - Verwerkersovereenkomst met eventuele verwerkers zijn aanwezig.

[4] I.v.m. controle op naleving van deze eis kan de Raad hierover nadere onderbouwende stukken opvragen welke dienen te worden overlegt.
[5] (Uitvoeringswet) Algemene Verordening Gegevensbescherming ((U)AVG), Wet Justititiële en Strafvorderlijke gegevens (Wjsg), Wet Politiegegevens (Wpg)
[6] Zie ook website Autoriteit Persoonsgegevens: Data protection impact assessment (DPIA) | Autoriteit Persoonsgegevens

Op basis van de AVG moet het product of dienst aan alle vereisten in de checklist van de Autoriteit Persoonsgegevens worden voldaan. De privacy vereisten moeten worden toegelicht aan de hand van onderbouwende documentatie.

(vi) Monitoring en verantwoording

- Periodiek wordt een overzicht gegeven van aantallen gebruikers en afhakers.
- Periodiek worden de resultaten van het klanttevredenheidsonderzoek gegeven.
- Periodiek wordt een overzicht gegeven van aantal klachten en wijze van afhandeling.
- (Indien een subsidieregeling van toepassing is) Bij gebruik van de subsidieregeling worden ter controle van de rechtmatigheid de NAW-gegevens en benodigde andere gegevens van de gebruiker verstrekt aan de Raad.
- (Indien een subsidieregeling van toepassing is) Periodiek worden data verstrekt aan de Raad voor de Monitor gesubsidieerde rechtsbijstand en ander onderzoek dat in het kader van de taakstelling van de Raad wordt uitgevoerd over het gebruik van het product/dienst door gebruikers die binnen de subsidieregeling vallen.

(vii) Rechtsbescherming

Besluiten tot verlening of afwijzing van de toelating alsmede besluiten tot verlenging of intrekking ervan zijn voor bezwaar en beroep vatbare beslissingen die onder de rechtsbescherming van de Awb vallen. Besluiten tot verlenging, afwijzing, intrekking en terugvordering van startsubsidies vallen eveneens onder de reikwijdte van de Awb. Omdat aan de Raad beleidsvrijheid toekomt met betrekking tot deze besluiten zal de toetsing marginaal zijn. Besluiten mogen evenwel niet in strijd komen met de algemene beginselen van behoorlijk bestuur.