bijlage 2:
checklist informatiebeveiliging voor leveranciers van clouddiensten

1. Met de leverancier wordt een verwerkers-, zelfstandig-, of gezamenlijke verantwoordelijken overeenkomst afgesloten indien de leverancier persoonsgegevens verwerkt. Het model van de IBD wordt hiervoor gebruikt.

2. De leverancier heeft een ISO 27001 of vergelijkbaar certificaat dat door een geaccrediteerde partij is afgegeven. Een ISAE3402 type 2, SOC 1 of SOC 2 certificering is wenselijk is. Daarnaast strekt ook een ISO 27017 of ISO 27018 certificering tot aanbeveling.

3. De leverancier stelt een kopie van het certificaat genoemd onder 2) ter beschikking van de gemeente.

4. Indien de leverancier geen ISO 27001 certificering heeft toont de leverancier aan op welke wijze de verwerking van de gegevens van de gemeente Houten ISO of BIO compliant is (BIO = Baseline Informatiebeveiliging Overheid). Dit kan bijvoorbeeld door aansluiting bij de gedragscode ***Data Pro Code*** van NLdigital. Deze gedragscode is goedgekeurd door de Autoriteit Persoonsgegevens.

5. De leverancier geeft voor in ieder geval de standaarden HTTPS/TLS, SAML, en security.txt van *Forum Standaardisatie* aan of ze zijn toegepast of dat gemotiveerd is afgeweken: 'Pas toe leg uit' standaarden (verplicht) | Forum Standaardisatie.

6. Toegang tot de gegevens wordt geregeld via het toegangsbeleid van de gemeente Houten (IP restricted of SSO op basis van Azure AD én minimaal 2-factor authenticatie).

7. Gegevens op transport, in verwerking of in rust behoort tijdens transport en in rust te worden beschermd op basis van sterke, ‘state of the art’ cryptografie.

8. Gegevens dienen te allen tijde binnen de rechtsmacht en juridische context van de Nederlandse wetgeving te blijven. Dit geldt ook voor subverwerkers van de verwerker.

9. Gegevens van de gemeente Houten worden niet verwerkt in de Verenigde Staten van Amerika.

10. Een eventuele moedermaatschappij van de leverancier gevestigd in de Verenigde Staten van Amerika heeft geen toegang tot de gegevens van de gemeente Houten.

11. Gegevens van de gemeente Houten behoren tijdens transport, bewerking en opslag, duurzaam geïsoleerd te zijn van de onderliggende dienstverlening, beheerfuncties en gegevens, die de leverancier voor andere klanten in beheer heeft.

12. De leverancier is verantwoordelijk voor het aanvragen van een VOG voor medewerkers die toegang krijgen tot gegevens van de gemeente Houten.

13. Medewerkers van de leverancier behoren alleen toegang te krijgen tot IT-diensten en gegevens waarvoor zij specifiek bevoegd zijn. Om dit aan te tonen kan de leverancier een autorisatiematrix aanleveren.

14. Toegang tot bijzondere persoonsgegevens (volgens art. 9 AVG) is verboden, tenzij dit plaatsvindt op basis van een wettelijke plicht, of expliciet door de gemeente Houten is toegestaan.

15. In ontwikkel-, test-, en acceptatie omgevingen worden geen persoonsgegevens gebruikt, maar wordt gewerkt met dummy data.

16. Logging vindt plaats volgens de aanwijzingen en handreikingen van de Baseline Informatiebeveiliging Overheid (*BIO-v1.0.4, Hfst 9.4.4, Speciale systeemhulpmiddelen, én Hfst 12.4 Verslaglegging en Monitoren*).

17. Ter bescherming tegen malware behoren beheersmaatregelen voor detectie, preventie en herstel te worden geïmplementeerd, waaronder regelmatige pentesten, in combinatie met een passend bewustzijn van medewerkers van de cloud leverancier.

18. Kritische bedrijfsprocessen bij de leverancier behoren te worden gefaciliteerd door een technische infrastructuur, die robuust is, fout-tolerant en voorzien is van ingebouwde herstelfuncties die periodiek worden getest.

19. Informatieverwerkende faciliteiten behoren met voldoende redundantie te worden geïmplementeerd om aan beschikbaarheidseisen te voldoen.

20. De belangrijkste processen zoals back-up en recovery, wijzigingsbeheer en incidentafhandeling zijn ingericht conform ITIL en onderdeel van de SLA.

21. Met de leverancier wordt in een SLA inzichtelijk gemaakt wat de beschikbaarheid van de clouddienst is over de hele keten, inclusief bij sub-verwerkers waar software en data worden gehost.

22. Periodiek (kwartaal of halfjaarlijks) wordt er gerapporteerd over beveilingsincidenten. Geef hieronder aan hoe de gemeente Houten hierover wordt ingelicht (bijvoorbeeld via een beheerdersnieuwsbrief, via een klantportaal, etc.).

23. *Optioneel, alleen op speciaal verzoek van de gemeente Houten*: Met de cloud leverancier wordt een Saas-escrow en een continuïteitsregeling afgesproken. Met een continuïteitsregeling wordt gegarandeerd dat de dienstverlening wordt voorgezet bij problemen bij de cloud leverancier totdat een structurele oplossing voor de gemeente Houten is gevonden.

24. In een clouddiensten overeenkomst wordt een Exit strategie opgenomen waarbij zowel een bepalingen aangaande exit als condities die aanleiding kunnen geven tot exit zijn opgenomen.

25. De leverancier voorziet in de mogelijkheid van dataportabiliteit.

26. De leverancier is bereid om, indien daaraan behoefte bestaat bij de gemeente Houten, periodiek een audit te laten uitvoeren en de gemeente Houten, tegen een redelijke vergoeding van de kosten, van het resultaat daarvan middels een TPM op de hoogte te stellen.

27. Security patches worden zo snel mogelijk, maar uiterlijk binnen een week geïnstalleerd. In de tussentijd worden op basis van een expliciete risicoafweging mitigerende maatregelen getroffen. ***Kritieke*** security patches worden binnen 48 uur na verschijning geimplementeerd.

28. De gangbare principes rondom Privacy by Design en Security by design zijn uitgangspunt voor de ontwikkeling van software en systemen geweest, én dit wordt door de leverancier aangetoond. Gangbare Privacy by Design principes zijn te vinden in ***The Little Blue Book***, van Jaap-Henk Hoepman[1].

29. Indien sprake is van ontwikkeling van een website of toegang tot de cloudapplicatie via een webportaal dient deze te voldoen aan de meest actuele webrichtlijnen (momenteel WCAG 2.1, niveau A en AA).

[1] https://www.cs.ru.nl/~jhh/publications/pds-booklet.pdf