

Algemene eisenlijst Privacy & Beveiliging

1. De organisatie van de Opdrachtnemer en zijn dienstverlening dienen in opzet, bestaan en werking te voldoen aan hoofdstuk 1 van de Baseline Informatiebeveiliging Overheid (BIO, versie 1.04, te downloaden op www.bio-overheid.nl) en toont dat jaarlijks aan middels onafhankelijke onderzoeken. Over deze onderzoeken brengt de Opdrachtnemer jaarlijks een assurance-verklaring uit aan de Opdrachtgever.
2. Opdrachtnemer heeft een beveiligingsfunctie benoemd en een beveiligingsorganisatie ingericht, waarin de organisatorische positie, de taken, verantwoordelijkheden en bevoegdheden van de betrokken functionarissen en de rapportagelijnen zijn vastgesteld.
3. Informatiebeveiliging en privacy zijn dynamische onderwerpen. Opdrachtnemer houdt de maatregelen vanwege toenemende risico's en bedreigingen via een PDCA-cyclus actueel.
4. De Opdrachtgever heeft het recht om maximaal een maal per jaar een audit te laten uitvoeren. Deze audit wordt in overleg met de Opdrachtnemer ingepland.
5. De eisen zijn ook van toepassing op onderaannemers van de Opdrachtnemer.
6. De organisatie van de Opdrachtnemer heeft van eenieder, die persoonsgegevens verwerkt of een verwerking voorbereidt, een actuele VOG, een actuele verklaring ter zake het naleven en de kennisname van de regels omtrent privacy en het bewijs van op de hoogte zijn van de disciplinaire procedure; hiervan bestaat een overzicht.
7. De organisatie van de Opdrachtnemer heeft de kennis georganiseerd om de oorzaak van een datalek te kunnen vaststellen en te onderzoeken, heeft daarvoor de benodigde loggegevens om herhaling te voorkomen en heeft de belanghebbenden vastgesteld om ze te kunnen informeren.
8. Het eigenaarschap en de verantwoordelijkheid voor logische toegangsbeveiligingssystemen en de verantwoordelijkheid voor fysieke toegangsbeveiligingssystemen is door de Opdrachtnemer vastgelegd.
9. Een formele registratie- en afmeldprocedure voor medewerkers van de Opdrachtnemer dient te zijn geïmplementeerd om toewijzing van toegangsrechten mogelijk te maken.
10. Een formele gebruikerstoegangsverleningsprocedure voor medewerkers van de Opdrachtnemer dient te zijn geïmplementeerd om toegangsrechten voor alle typen gebruikers en voor alle systemen en diensten toe te wijzen of in te trekken.
11. Opdrachtnemer zorgt ervoor dat de toegang tot systemen en toepassingen wordt beheerst door een beveiligde inlogprocedure. Hiervan dient verificatie in meerdere stappen onderdeel uit te maken als het inloggen plaatsvindt vanaf een niet vertrouwde locatie en over een niet vertrouwd netwerk.
12. Opdrachtnemer zorgt voor systemen voor wachtwoordbeheer die interactief zijn en sterke wachtwoorden waarborgen.
13. Opdrachtnemer beperkt en beheerst de toewijzing en gebruik van speciale toegangsrechten.
14. Opdrachtnemer scheidt binnen zijn organisatie conflicterende taken en verantwoordelijkheden om de kans op onbevoegd of onbedoeld wijzigen of misbruik van bedrijfsmiddelen te verminderen.
15. Opdrachtnemer beheerst het toewijzen van geheime authenticatie-informatie door middel van een formeel beheersproces.

16. Ter ondersteuning van autorisatiebeheer biedt Opdrachtnemer, binnen de applicatie, technische autorisatievoorzieningen, zoals: een personeelsregistratiesysteem, een autorisatiebeheersysteem en autorisatiefaciliteiten.
17. Binnen de gebouwen van de Opdrachtnemer en onderaannemers worden beveiligde gebieden beschermd door passende toegangsbeveiliging om ervoor te zorgen dat alleen bevoegd personeel toegang krijgt.
18. Opdrachtnemer controleert het gebruik van toegangsbeveiligingsvoorzieningen volgens vastgestelde procedures.
19. Opdrachtnemer maakt log-bestanden van gebeurtenissen die gebruikersactiviteiten, uitzonderingen en informatiebeveiligingsgebeurtenissen registreren, en stelt deze op verzoek aan de opdrachtgever ter beschikking zodat ze kunnen worden beoordeeld.
20. Opdrachtnemer zorgt voor het loggen op verwerkers/persoonsniveau, zodat direct of periodiek kan worden beoordeeld welke persoonsgegevens de medewerker heeft opgevraagd, ingezien en aangepast.
21. Het verlenen van toegang tot persoonsgegevens aan medewerkers van de opdrachtnemer wordt beperkt op basis van duidelijke en afgebakende taken en het doel en de verstrekte toegang is toetsbaar.
22. Opdrachtnemer zorgt er aan zijn kant voor dat IT-functionaliteiten worden verleend vanuit een robuuste en beveiligde systeemketen van de opdrachtnemer naar de opdrachtgever.
23. Opdrachtnemer heeft het netwerk, waarin de aangeboden applicatie is geïnstalleerd en de hierin verwerkte gegevens zijn opgeslagen, gescheiden in logische en fysieke domeinen (zones). In het bijzonder is er een Demilitarized Zone (DMZ) die tussen het interne netwerk en het internet gepositioneerd.
24. Opdrachtnemer heeft voor alle hard en software, betrokken bij de aangeboden diensten, hardening toegepast met de meest actuele en bewezen technieken.
25. Opdrachtnemer heeft informatie-verwerkende faciliteiten met voldoende redundantie geïmplementeerd om aan continuïteitseisen te voldoen.
26. Opdrachtnemer faciliteert de herstelfunctie van data en clouddiensten, gericht op ondersteuning van bedrijfsprocessen, met infrastructuur en IT-diensten, die robuust zijn en periodiek worden getest.
27. Opdrachtnemer beschermt data tijdens transport, verwerking en in opslag met cryptografie-maatregelen in overeenstemming met Nederlandse wetgeving.
28. Gearchiveerde data slaat de opdrachtnemer gedurende de overeengekomen bewaartermijn, technologie-onafhankelijk, raadpleegbaar, onveranderbaar en integer op vernietigt deze op aanwijzing van de Opdrachtnemer.
29. De cloud-infrastructuur is door de Opdrachtnemer zodanig ingericht dat de dienstverlening aan gebruikers van informatiediensten is gescheiden.
30. Opdrachtnemer zorgt er voor dat gegevens van de Opdrachtgever tijdens transport, bewerking en opslag duurzaam geïsoleerd zijn van beheerfuncties en data van andere klanten, die de CSP in beheer heeft.
31. Opdrachtnemer implementeert beheersmaatregelen tegen malware voor detectie, preventie en herstel in combinatie met een passend risicobewustzijn bij de eigen medewerkers.
32. Opdrachtnemer bewaakt en beheerst onderlinge netwerkconnecties (koppelvlakken) in de keten van de opdrachtgever naar de Opdrachtnemer om de risico's van datalekken te beperken.
33. Opdrachtnemer gebruikt als testdata alleen kunstmatig gegenereerde persoonsgegevens of fictieve data.
34. De, door Opdrachtnemer aangeboden, applicatie biedt de mogelijkheid om op aangeven van betrokkene, waarvan de persoonsgegevens worden verwerkt, controle te houden over de gegevens en de verwerking ervan, zodat de juistheid en nauwkeurigheid van de

gegevens kan worden gewaarborgd en de verwerking ervan kan worden gecorrigeerd, gestaakt of overgedragen.

35. De Opdrachtnemer heeft maatregelen getroffen die voorkomen dat de uitval van een dienst, of dit nu een eigen dienst is of van een derde is, leidt tot een datalek of andere gevolgen voor betrokkenen, waarvan de persoonsgegevens worden verwerkt, en heeft een procedure om de werking van de maatregel te evalueren.
36. De Opdrachtnemer garandeert jaarlijks inzage in de resultaten van een penetratietest, uitgevoerd door een derde onafhankelijke partij.