# Acceptatiecriteria ICT-systemen

## Informatiebeveiliging
## &
## gegevensbescherming

Auteurs : Helma de Boer, René Dol, Hans Hoeven

**Colofon**

In deze notitie staan de 'generieke' eisen genoemd waar de door Deltion gebruikte ICT-systemen en de betrokken opdrachtnemers aan moeten voldoen op het gebied van informatiebeveiliging en gegevensbescherming.

**Samenstelling en beheer**



## Versiebeheer

*OA2007-0008*

| Versie | Door | Datum | Wijziging/actie |
|---|---|---|---|
| 0.1 | René Dol, Hans Hoeven, Helma de Boer | 08-04-2020 | Initieel document |
| 0.2 | René Dol, Rob Vos | 17-04-2020 | Minor tekstuele aanpassingen |
| 0.3 | Helma de Boer | 20-04-2020 | Opmerkingen verwerkt, verbetering kleine spelfouten |
| 0.4 | René Dol | 23-06-2020 | Bijstellen tijdens bespreking Hans, Helma, Sietze |
| 0.5 | René Dol, Hans Hoeven, Helma de Boer | 24-06-2020 | concept |
| 1.0 | Helma de Boer | 29-06-2020 | Versie 1.0 - goedgekeurd/vastgesteld RV/JK |
| 1.1 | Helma de Boer | 01-10-2020 | Actualisering i.v.m. Schrems II/Privacy Shield |
| 1.2 | Rene Dol | 28-10-2020 | Integratie van eisen genoemd in notitie Basiseisen websites Deltion. |
| 1.3 | Rene Dol | 23-11-2020 | Toegevoegd responsible disclosure |
| 1.4 | Helma de Boer | 01-12-2020 | Toegevoegd MFA smartphone-app (toegangscode) |
| 1.5 | Rene Dol | 10-02-2021 | Toegevoegd e-mailbeveiling |
| 1.6 | *Helma de Boer* | 01-03-2021 | Dubbeling authenticatie eruit, taalkundige verbeteringen |

## Inhoudsopgave

# 1. Inleiding

In deze notitie staan de 'generieke' eisen genoemd waar de door Deltion gebruikte ICT-systemen en de betrokken opdrachtnemers aan moeten voldoen op het gebied van informatiebeveiliging en gegevensbescherming.

Deze notitie verwoordt geen uitspraken over eigenaarschap van systemen, processen en gegevens en de geboden functionaliteit van de applicatie.

Onder de definitie 'Opdrachtnemer' zoals in deze notitie wordt gehanteerd, kunnen verschillende partijen worden verstaan, afhankelijk van de context van de genoemde criteria. Denk aan softwareontwikkelaar, verkopende partij, opdrachtnemer, dienstverlener (SAAS-partij), verwerker in de zin van de AVG, de hostingpartij, etc.

Dit document kan gebruikt worden als checklist en biedt ook een globaal/vereenvoudigd overzicht van hetgeen meer in detail en formeel is vastgelegd in onderliggende beleidstukken op het gebied van hardening, encryptie, autorisaties, enz. Bij tegenstrijdigheden geldt het onderliggende beleid.

# 2. Criteria voor dienstverlening en dienstverlener

## 2.1 Incidentmanagement

Voor het oplossen van incidenten is een incidentenbeheerproces ingericht (conform ITIL of gelijkwaardig). Er zijn geen generieke eisen waar dit proces aan moet voldoen. Dit varieert per applicatie(dienst). Denk aan responsetijden, openingstijden.

## 2.2 Beschikbaarheid, performance & capaciteit

| | | |
|---|---|---|
| De beschikbaarheid | : | deze is in overeenstemming met de (te verwachten) risicoscores (BIV). |
| De performance | : | hiervoor zijn geen generieke eisen. |
| De capaciteit | : | hiervoor zijn geen generieke eisen. |

## 2.3 Contractvoorwaarden

De opdrachtnemer accepteert de Deltion-inkoopvoorwaarden.

## 2.4 Eigenaarschap gegevens

Deltion is eigenaar van haar gegevens in de applicatie.

## 2.5 Responsible disclosure

De leverancier meldt Deltion gevonden zwakheden in de informatiebeveiliging of gegevensbescherming (AVG) op een wijze vergelijkbaar met de responsible disclosure-regeling van Deltion (zie de openbare Deltion-website).

## 2.6 Exit-overeenkomst

Na afloop van de dienstverlening of overeenkomst:

- zijn alle Deltion-gegevens beschikbaar
- in een gangbaar door Deltion bruikbaar formaat
- binnen 1 week na een door Deltion ingediend verzoek
- worden op verzoek alle Deltion-gegevens definitief vernietigd

### 2.7 Continuïteit dienstverlening

De opdrachtnemer biedt voor de geboden dienst en/of het product voldoende waarborgen voor continuïteit. Denk aan marktaandeel, financiële situatie van het bedrijf, toekomstvastheid van het product.

## 3. Criteria voor architectuur

Het systeem voldoet aan de gewenste inrichting en samenhang van de architectuur van het Deltion-applicatie-landschap.

Het systeem voldoet aan de architectuurprincipes van Deltion.

## 4. Criteria voor gegevensbescherming (AVG)

Het systeem voorziet in Privacy by Design zoals bedoeld in de AVG (waaronder anonimiseren, dataminimalisatie, pseudonimiseren, encryptie, access control, Privacy by Default, bewaren/vernietigen, faciliteren rechten betrokkenen, beheer).

Persoonsgegevens worden opgeslagen in de EU/EER. Opslag in een land daarbuiten is alleen toegestaan bij passende waarborgen (houd er rekening mee dat Privacy Shield en standaard contractuele clausules niet meer bruikbaar zijn voor Amerikaanse leveranciers).

De door Deltion gehanteerde bewaar- en vernietigingstermijnen kunnen via de applicatie worden gehandhaafd.

De opdrachtnemer draagt bij einde dienstverlening alle gegevens over aan Deltion en/of vernietigt deze en bewaart geen gegevens voor eigen doeleinden.

Er wordt multifactorauthenticatie (MFA) toegepast als er bijzondere persoonsgegevens worden opgeslagen. In het geval van een smartphone-app is dat via een ingebouwde toegangscode (zoals bij een bankieren-app).

Het autorisatiebeheer kan afdwingen dat gebruikers alleen toegang hebben die tot informatie die strikt nodig is voor hun werkzaamheden (need-to-know, time-to-know, least privilege).

De verwerker is bereid een door Deltion goedgekeurde verwerkersovereenkomst te ondertekenen.

De verwerker verwerkt zonder toestemming geen gegevens van Deltion voor eigen doelen (zoals testen en data-analyses).

De aansprakelijkheid op basis van de AVG voor boetes van de Autoriteit Persoonsgegevens en voor schadevergoeding van gedupeerden door nalatigheid/toerekenbaarheid van de verwerker, wordt niet beperkt.

Als een applicatie toegang nodig heeft tot een werkstation (zoals een laptop of smartphone), dan is die toegang beperkt tot wat nodig is om de functionaliteit te bieden waarvoor de applicatie is bedoeld.

Als een applicatie voor smartphone/tablets beschikbaar is gesteld als app, is er ook een web-based alternatief met de benodigde functionaliteit beschikbaar (smartphone-app is optioneel).

De opdrachtnemer hanteert een normenkader voor informatiebeveiliging, zoals ISO 27001, ROSA, etc. zowel voor logische als fysieke beveiligingsmaatregelen.

Het systeem biedt de mogelijkheid om het verwerken van persoonsgegevens die niet strikt noodzakelijk zijn, te voorkomen bijvoorbeeld door functionaliteit uit te schakelen (dataminimalisatie).

Het systeem (in het geval van een Deltion-website) verwijst met een link naar de privacyverklaring van Deltion.

Alle in- en uitvoer van data wordt genormaliseerd, gevalideerd en ingeperkt om de data-integriteit te waarborgen, bijvoorbeeld door beveiliging van invoervelden tegen misbruik zoals SQL-injection en XSS en beveiliging tegen misbruik van bestanden via macro's.

Het systeem voorziet in logging van kritische handelingen (zoals het aanmaken van accounts, het bewerken en verwijderen van persoonsgegevens, etc.).

Een website bevat bij voorkeur alleen functionele cookies wenselijk voor de juiste werking van de applicatie. Cookies voor marketingdoeleinden (first en third party) worden alleen actief na een opt-in keuze met transparantie over doel en gebruik.

# 5. Criteria m.b.t. informatiebeveiliging

## 5.1 Informatiebeveiligingsbeleid

De opdrachtnemer heeft informatiebeveiliging aantoonbaar professioneel ingericht en zit gemiddeld op volwassenheidsniveau 2,5 conform O-ISMS (open information security maturity model).

De opdrachtnemer meldt ernstige informatiebeveiligingsincidenten direct aan Deltion en neemt zo snel mogelijk maatregelen om de gevolgen en de schade te beperken.

De opdrachtnemer stelt Deltion direct op de hoogte van risico's die niet afdoende door mitigerende maatregelen zijn beperkt.

De opdrachtnemer controleert minimaal eens per jaar de toegangsrechten van de eigen medewerkers en minimaliseert die tot het strikt noodzakelijke.

Alle medewerkers van de opdrachtnemer hebben een geheimhoudingsplicht.

Alle medewerkers van de opdrachtnemer hebben uitsluitend toegang tot Deltion-gegevens voor zover noodzakelijk voor het leveren van de dienst.

Opdrachtnemer overlegt met Deltion voordat gegevens aan derden worden verstrekt (zoals justitie).

## 5.2 Versleuteling

Alle gegevens worden via een versleutelde verbinding getransporteerd.

Alle gegevens die in bestanden, databanken zijn opgeslagen, zijn versleuteld waar zinvol en mogelijk.

Alle opgeslagen accountgegevens zijn versleuteld.

De TLS- en SSL-versleuteling voldoet aan de NCSC ICT-Beveiligingsrichtlijnen dan wel gelijkwaardige richtlijnen zoals OWASP.

## 5.3 Sessiebeheer

Er is sessiemanagement ingericht om misbruik van bestaande sessies tegen te gaan volgens de richtlijnen van OWASP of gelijkwaardig, (https://www.owasp. org/index.php/Testing_for_Session_Management_Schema_(OTG-SESS-001).

## 5.4 E-mail beveiliging

Bij versturen van e-mailberichten zijn er anti-spam maatregelen genomen zoals het gebruikmaken van SPF-, DKIM- en DMARC-techniek.

## 5.5 Back-up

Alle gegevens in de applicatie zijn opgenomen in een back-up. De frequentie en de omvang hiervan zijn in overeenstemming met de (te verwachten) risicoscores (BIV).

De back-up wordt op een veilige locatie opgeborgen; fysiek gescheiden van de productielocatie.

## 5.6 Restore

De omgeving (applicatie en gegevensbestanden) kan worden hersteld na een calamiteit. De omvang en snelheid hiervan zijn in overeenstemming met de (te verwachten) risicoscores (BIV).

## 5.7 OTAP-omgeving

Een test- en/of acceptatie-omgeving bevat geen persoonsgegevens uit de productieomgeving.

## 5.8 Huisvesting

De huisvesting van de IT-systemen is professioneel ingericht volgens gangbare normen in dit werkveld. Dit omvat minimaal maatregelen voor inbraak, stroomuitval, koeling, waterschade, toegangsbeheer.

## 5.9 Hardening

De gegevens van Deltion zijn logisch of fysiek afgeschermd van partijen die die gegevens niet mogen inzien. Denk aan het scheiden van databanken tussen de diverse afnemers van een SAAS-dienst.

Alle betrokken ICT-componenten zijn veilig ingericht/geconfigureerd (security hardening) op basis van in de branche gebruikelijke best practise-maatregelen.

Het afluisteren en ingrijpen in netwerkverbindingen en datastromen wordt verhinderd door de toepassing van in de branche gebruikelijke best practise-maatregelen.

Het lekken van configuratiegegevens in headers, banners en error-pagina's moet worden voorkomen.

ICT-componenten worden bij voorkeur dagelijks en minimaal wekelijks op kwetsbaarheden (vulnerability- en patchmanagement) gecontroleerd. Opdrachtnemer neemt zo snel mogelijk mitigerende maatregelen. Als die maatregelen de risico's niet snel genoeg of niet afdoende beperken dan informeert opdrachtnemer de opdrachtgever tijdig.

Webapplicaties zijn beveiligd conform de richtlijnen van de NCSC (ICT-Beveiligingsrichtlijnen voor Webapplicaties) of gelijkwaardig. Dit omvat minimaal de door OWASP genoemde top tien maatregelen voor webapplicaties (https://owasp.org/www-project-top-ten/).

## 5.10 Logging

Kritieke handelingen van gebruikers (zoals wijzigingen van autorisaties, goedkeuren van een examen, wissen van belangrijke gegevens, toegang tot gevoelige gegevens) worden gelogd en zijn inzichtelijk/opvraagbaar voor beheerders.

De loggegevens zijn beveiligd tegen ongeautoriseerde toegang en/of wijziging en zijn niet te verwijderen door de normale gebruikers (niet zijnde systeem- of applicatiebeheerders).

## 5.11 Authenticatie – Autorisatie – ILM

Het authenticeren (inloggen) gaat in overeenstemming met de (te verwachten) risicoscores (BIV). Denk aan de toepassing van multifactorauthenticatie (MFA).

Het systeem controleert op het gebruik van sterke wachtwoorden en slaat deze gehasht op.

De authenticatievoorzieningen kunnen gebruikmaken van of zijn compatible met de door Deltion gebruikte of goedgekeurde authenticatievoorzieningen (zoals SURFConext, ADFS en in de toekomst Azure-AD e.d.).

Het autorisatiebeheer vindt plaats op basis van rollen waarmee kan worden afgedwongen dat gebruikers alleen toegang hebben tot die tot informatie die strikt nodig is voor hun werkzaamheden (need-to-know, time-to-know, least privilege).

Het autorisatiebeheer kan bij voorkeur gebruikmaken van de status van gebruikers in de Deltion-bronsystemen.

Het identiteitenbeheer (Identity Lifecycle Management) kan plaatsvinden via automatische provisioning via doel- en bronsystemen van Deltion.

## 5.12 Koppelingen

De applicatie kan waar nodig geautomatiseerd gegevens uitwisselen met de Deltion-middlewarelaag.

## 5.13 Inpasbaarheid Deltion-infrastructuur

Als (delen van) het systeem on premise wordt gehost, dan past dit in de infrastructuur van Deltion voor wat betreft de of het gebruikte:

- besturingssysteem is bij voorkeur MS Windows;
- databasemanagementsysteem is bij voorkeur MS SQL-server;
- webserverplatform is bij voorkeur MS IIS;
- beheertools voor servermanagement, dit moet met MS Managementconsole, MS SCCM kunnen.
- de gebruikte beheeromgeving voor monitoring, dit moet mogelijk zijn SNMP, WMI, SSH, Powershell en/of serviceaccount;
- oplossing voor remotebeheer, dit moet met MS RDP via een VPN kunnen;
- back-up- en restore-programmatuur, dit moet met MS DPM kunnen;
- servervirtualisatie, dit moet met MS HyperV kunnen;
- storage-omgeving (NAS/SAN), dit moet met de Deltion Dell-storage omgeving kunnen.
- deployment-oplossing; dit moet met MS SCCM en/of Scense (AppiXoft) kunnen;

- ondersteuning voor SNMP; dit moet minimaal SNMPv2 zijn; bij voorkeur SNMPv3
- netwerkkoppelvlak; dit moet standaard UTP of SFP zijn.

Voor bovenstaande systemen geldt dat de systemen qua versie niet verouderd zijn en up-to-date zijn voor wat het doorvoeren van security-patches betreft.