



## Security en Privacy

De beveiliging van persoonsgegevens en bedrijfsgevoelige informatie kan sinds een aantal jaren gelukkig rekenen op ruime aandacht van overheden en leveranciers. Het grote aantal meldingen van datalekken, de forse toename van slachtoffers van identiteitsfraude, de voortdurende dreiging van cyberaanvallen en de geslaagde gijzelingen met ransomware laten zien dat die aandacht meer dan terecht is.

Als leverancier van softwareproducten en diensten als verwerker heeft Centric in de afgelopen jaren maatregelen getroffen voor de beveiliging van gevoelige gegevens. Met deze maatregelen helpen wij onze klanten te voldoen aan de eisen van wet- en regelgeving zoals de Algemene verordening gegevensbescherming (AVG), het normenkader ICT-beveiligingsassessment DigiD, de Baseline Informatiebeveiliging Overheid (BIO) en de Eenduidige Normatiek Single Information Audit (ENSIA). Dit vanzelfsprekend in combinatie met de interne maatregelen die nodig zijn.

Nieuwe wet- en regelgeving maar ook nieuwe dreigingen vereisen steeds weer aanvullende beveiligingsmaatregelen. De BIO met bijbehorende handreikingen en thema-uitwerkingen is een voorbeeld van vernieuwde regelgeving. Het beveiligen van onze softwarediensten is daarom geen eenmalige actie, maar een belangrijk onderdeel van ontwikkeling, dienstverlening en beheer. Omdat Centric steeds meer opereert als cloudserviceprovider, mogen onze klanten verwachten dat we ook proactief onze verantwoordelijkheid nemen om de data van klanten in onze omgevingen optimaal te beveiligen.

Eind 2021 heeft Centric samen met de Gebruikersvereniging een vakgroep Informatiebeveiliging en Privacy in het leven geroepen. De groep bestaat uit CISO's, FG's, Security Officers en Privacy Officers vanuit het hele land en vertegenwoordigen zowel de kleinere klanten als de grotere klanten. In de bijeenkomsten komen allerlei onderwerpen aan bod, wat ervoor zorgt dat Centric scherp blijft op de uitdagingen waar onze gebruikers zoal tegenaan lopen. Zo kunnen we oplossingen bieden die aansluiten op de behoeften van de klant. Eén van die behoeften is om een digitaal weerbare organisatie te zijn.

Naast het waarborgen van security en privacy binnen onze producten en diensten heeft Centric de ambitie in de komende jaren een breder producten- en dienstenportfolio op te bouwen waarmee wij klanten ondersteunen op het gebied van Security & Privacy. Zie hiervoor ook het onderdeel Security & Privacy onder het aandachtsgebied Informatiebeleid.

De volgende paragrafen beschrijven hoe Centric invulling geeft aan het beleid voor informatiebeveiliging en de maatregelen we nemen om de beschikbaarheid, integriteit en vertrouwelijkheid te waarborgen voor onze producten en diensten. Meer informatie over hoe Centric omgaat met de thema's Security en Privacy vindt u in ons Centric Trust Center.

## Security

### Centric beleid informatiebeveiliging

Centric heeft een informatiebeveiligingsbeleid opgesteld waarin de uitgangspunten en stuurmechanismen benoemd zijn voor een veilige verwerking van gegevens. Het beleid is uitgewerkt in concrete procedures en maatregelen en is van toepassing voor alle Centric-medewerkers.

### Secure Software Development

De basis voor security ligt bij de ontwikkeling van veilige software. Centric gebruikt hiervoor de methode en normenkaders van Secure Software Development (SSD) van het [Centrum Informatiebeveiliging en Privacybescherming \(CIP\)](#). Wij passen daarbij de methode [Grip op SSD](#) toe. Hierdoor hebben klanten inzicht in onze werkwijze voor het ontwikkelen van veilige software. Centric heeft actief bijgedragen aan vernieuwing van de SSD-normen, versie 3. De security requirements van SSD zijn opgenomen in de Centric Baseline voor secure software development en zijn voorwaarde bij de (door)ontwikkeling van onze software.

## Security audits en pentesten

Centric heeft een eigen team van ethische hackers (het Red Team) die structureel security audits en pentesten uitvoeren op onze softwareproducten en -diensten. Bij het testen wordt onder andere gebruik gemaakt van de SSD-normenkaders, de Top 10 Application Security Risks van [Open Web Application Security Project \(OWASP\)](#), de [Nationaal Cyber Security Centrum \(NCSC\)](#) ICT-Beveiligingsrichtlijnen voor Webapplicaties en mobiele applicaties en andere CVE's (Common Vulnerabilities and Exposures). De bevindingen van deze pentests leiden tot aanpassingen binnen onze software. Voor het classificeren en prioriteren op basis van de (technische) ernst van de gevonden kwetsbaarheden wordt CVSS 3.1 aangehouden. CVSS staat voor Common Vulnerability Scoring System en ook dit is een open industriestandaard. Op basis van de zo bepaalde risico's en prioriteiten worden de kwetsbaarheden verholpen.

## DigiD-assessments

Logius vereist een jaarlijks ICT-beveiligingsassessment voor applicaties die DigiD gebruiken. Voor dit assessment heeft Logius een normenkader opgesteld. De toetsing moet worden uitgevoerd door een Register EDP-auditor. Voor de betreffende applicaties laat Centric jaarlijks een externe auditor een assessment uitvoeren voor het applicatiegedeelte en het hostingsgedeelte. De Third Party Mededeling (TPM) die we aan onze klanten ter beschikking stellen, dekt hiervoor relevante normen af. Ons streven is vanaf 2022 deze TPM uiterlijk 1 oktober aan onze klanten te leveren. Elke klant moet daarnaast een audit op het eigen securitybeleid laten uitvoeren. Onze TPM kan samen met het gedeelte van de klant bij Logius ter verificatie worden aangeboden.

## ISO 27001

Centric heeft voor de levering van (cloud)diensten een informatiebeveiligingsbeleid opgesteld en geïmplementeerd in lijn met de beveiligingsnorm ISO 27001. De beheeractiviteiten die worden uitgevoerd voor clouddiensten zijn volgens deze norm gecertificeerd. Op basis van jaarlijkse risicobeoordelingen, audits, wijzigingen in wet- en regelgeving en business requirements scherpen we ons informatiebeveiligingsbeleid continu aan. Centric verwacht begin 2022 ook de ISO 27001-certificering voor het softwareontwikkelproces te behalen, waarmee we aantoonbaar voldoen aan de eisen van de markt en toezichthouders. Voor 2022 geldt dat we de scope van deze certificering verder zullen uitbreiden. Uitbreiding van de ISO-certificering volgens 27002 en/of 27017 wordt hierbij ook overwogen.

## Privacy

Na het van kracht worden van de AVG in mei 2018 is er meer duidelijkheid ontstaan over de interpretatie en invulling van deze privacywet. Centric heeft in samenwerking met de Privacy Company een Centric Baseline Product Privacy opgesteld. Hierbij is gebruikgemaakt van het [Privacy by Design Framework](#) van de Privacy Company. Deze baseline is gebruikt om de bestaande applicaties te toetsen op overeenstemming met de AVG. Naar aanleiding van de bevindingen hieruit zijn aanpassingen doorgevoerd. Ook bij nieuwe ontwikkelingen stellen we met behulp van deze baseline de privacyeisen vast. Ook heeft Centric bijgedragen aan de totstandkoming van de [Privacy by Design-instrumenten](#) van de Informatiebeveiligingsdienst (IBD).

De AVG stelt rechtmatigheid, behoorlijkheid en transparantie bij de verwerking van persoonsgegevens voorop. Gegevens mogen uitsluitend worden verwerkt in het kader van een gerechtvaardigd doel en dan ook alleen die gegevens die strikt noodzakelijk zijn. Ook mogen gegevens niet langer bewaard blijven dan nodig. Daarnaast hebben rechthebbenden het recht om te weten welke gegevens er over hen bekend zijn en welke verwerkingen er hebben plaatsgevonden. Verder onderzoekt Centric de meerwaarde van ISO 27701 en/of 27018-certificering.

## Verwerkersovereenkomst

De AVG schrijft voor dat bij de verwerking van persoonsgegevens door een verwerker (in dit geval Centric) de afspraken en maatregelen om een veilige verwerking te garanderen worden vastgelegd in een verwerkersovereenkomst. Centric heeft meegewerkt aan de standaard verwerkersovereenkomst van de Vereniging van Nederlandse Gemeenten (VNG) en gebruikt de meeste recente versie (april 2021). Daarnaast heeft Centric meegewerkt aan het opstellen van een Factsheet om te bepalen in welke gevallen een leverancier een Verwerker is (in de zin van de AVG) en dat daarom een verwerkersovereenkomst moet worden afgesloten.

## Privacy statement

Centric heeft een privacyverklaring opgesteld. Behalve algemene zaken is hier informatie te vinden over specifieke verwerkingen die Centric voor haar klanten uitvoert in het kader van support en conversies.

## Monitoring van kwetsbaarheden en dreigingen

Om nieuwe kwetsbaarheden en mogelijke dreigingen continu te monitoren, maakt Centric onder andere gebruik van de dienstverlening Kwetsbaarheidswaarschuwingen van de Informatiebeveiligingsdienst (VNG/IBD). De IBD verzamelt informatie over aankomende of acute beveiligingsrisico's in software en hardware. Aangesloten gemeenten worden door de IBD geïnformeerd zodra zich bij hen een risico voordoet.

Om de diensten van de IBD optimaal te kunnen gebruiken, is het voor gemeenten van belang dat zij over de gewenste informatie beschikken. De gemeente is daarbij voor een deel afhankelijk van Centric als leverancier van software en eventuele clouddiensten (Hosting en SaaS). Met de IBD is afgesproken dat Centric informatie verstrekt over de gebruikte softwarecomponenten, IP-adressen en URL's. Het gaat hier om het publieke deel, dus de software en infrastructuur die vanaf het internet te benaderen of te gebruiken zijn. De afspraak met de IBD is dat de partijen elkaar zo snel mogelijk informeren over security- en privacy-incidenten en kwetsbaarheden. Op basis van een risicoanalyse nemen we passende maatregelen in software en hardware om daarmee de risico's te beperken.