Informatiebeveiligingsbeleid en gegevensbescherming CIZ t.b.v. aanbesteding onderhoud en ontwikkeling Portero en DWH

Datum: 24/06/2016

Versie: 0.3

Inhoud

1. Doel van dit document

In dit document wordt een samenhangend beeld geschetst van de wijze waarop het CIZ bij het uitvoeren van haar wettelijke taak zorg wil dragen voor de beveiliging van haar informatie in relatie tot de uit te besteden dienst omtrent ontwikkeling en onderhoud van Portero en Data Warehouse (DWH).

De eisen zijn zo veel mogelijk op beleidsniveau geformuleerd (richtinggevend) om de aanbieders de ruimte te bieden om hieraan naar eigen inzicht en expertise invulling te geven. Feitelijke eisen op operationeel niveau zijn niet opgenomen. Deze zullen later in de concretiseringsfase meegenomen worden.

2. Scope

Informatiebeveiligingsmaatregelen en eisen op het gebied van privacy van persoonsgegevens raken alle organisatieonderdelen, bedrijfsprocessen, systemen en informatiebronnen. Dit betekent dat de Applicatie-dienstverlener die het ontwikkelen en onderhouden van Portero en DWH uitvoert rekening zal moeten houden met deze aan het CIZ opgedragen wettelijke eisen op het gebied van informatiebeveiliging en bescherming van persoonsgegevens.

3. Definitie van informatiebeveiliging en privacy bescherming

Bij het uitvoeren van haar primaire taak verwerkt het CIZ veel bijzondere persoonsgegevens. Informatiebeveiliging neemt daarom bij het CIZ een belangrijke positie in, wat zich vertaald in een continu verbeterproces om de continuïteit van de bedrijfsvoering en de privacy van onze cliënten te waarborgen.
Onder informatiebeveiliging verstaat CIZ het waarborgen van de

- *Beschikbaarheid*
  Beschikbaarheid betreft het waarborgen dat geautoriseerde gebruikers op de juiste momenten toegang hebben tot informatie en aanverwante bedrijfsmiddelen (informatiesystemen).
- *Integriteit*
  Integriteit betreft het waarborgen van de juistheid, tijdigheid (actualiteit) en volledigheid van informatie en de verwerking ervan.
- *Vertrouwelijkheid*
  Met vertrouwelijkheid wordt gedoeld op het waarborgen dat informatie alleen toegankelijk is voor degenen die hiertoe zijn geautoriseerd.
- *Controleerbaarheid*
  Controleerbaarheid betreft de mogelijkheid om met voldoende zekerheid vast te kunnen stellen of wordt voldaan aan de eisen ten aanzien van beschikbaarheid, integriteit en vertrouwelijkheid.

De Wet bescherming persoonsgegevens (Wbp) bevat regels over het vastleggen en verstrekken van persoonsgegevens ter bescherming van de persoonlijke levenssfeer van de betrokkene. Dit betekent dat er o.a. aan de volgende regels voldaan zal moeten worden:

- Persoonsgegevens moeten op een zorgvuldige en behoorlijke wijze worden verwerkt, in overeenstemming met de wet (artikel 6 Wbp);
- De verwerking moet plaatsvinden met een rechtmatige grondslag (artikel 8 Wbp);
- Verdere verwerking van persoonsgegevens kan slechts plaatsvinden op grond van welbepaalde, uitdrukkelijk omschreven, gerechtvaardigde doelen (artikel 7, 9 en 43 Wbp);
- De kwaliteit van persoonsgegevens moet op orde zijn, ter zake dienend en niet bovenmatig (artikel 11 Wbp)
- Er moeten passende technische en organisatorische beveiligingsmaatregelen worden genomen om de persoonsgegevens te beschermen (artikel 13 Wbp);
- Waar nodig moeten afspraken met derden worden gemaakt over de verwerking van persoonsgegevens (artikel 14 Wbp);
- Persoonsgegevens mogen niet nodeloos (lang) worden bewaard (artikel 10 Wbp);

- De betrokkene heeft recht op informatie over de verwerking van zijn gegevens (artikel 33 en 34 Wbp);
- De betrokkene heeft recht op inzage, wijziging, verwijdering van de eigen persoonsgegevens (artikel 35, 36, 40-41 Wpb) en het recht om niet te worden onderworpen aan geautomatiseerde besluitvorming (artikel 42 Wbp);
- Aparte, strengere regimes voor de verwerking van bijzondere persoonsgegevens (artikel 16-23 Wbp) en gevoelige persoonsgegevens, waaronder wettelijke persoonsnummers (artikel 42 Wbp).

De Applicatie-dienstverlener heeft bij de ontwikkeling c.q. onderhoud van Portero en DWH voor het CIZ een significante rol en verantwoordelijkheid bij het implementeren van bovenstaande eisen op het gebied van het beschermen van persoonsgegevens. Tevens zal een aparte bewerkersovereenkomst worden afgesloten tussen de contractpartijen.

4. Kaders

CIZ is een ZBO en valt onder het ministerie van VWS en maakt daarbij dus ook deel uit van de Rijksoverheid. Naast algemene wetgeving heeft CIZ te voldoen aan kaders en richtlijnen die op deze plaats en rol binnen de overheid van toepassing zijn. Samen met haar eigen beleid resulteert dit in de volgende kaders op het gebied van informatiebeveiliging en privacybescherming:

Informatiebeveiliging

Wettelijk	Baseline Informatiebeveiliging Rijksdienst (BIR: 2012)
	Archiefwet
Regelgeving	Norm ICT-beveiligingsassessments DigiD
Handreikingen	OWASP top 10
	Software Improvement Group (SIG) – normen gebaseerd op ISO 25010
Intern beleid	Informatiebeveiligingsbeleid CIZ 2016

Privacy

Wettelijk	Wet bescherming persoonsgegevens (Wbp)
	Algemene Verordening Gegevensbescherming (AVG)
Regelgeving	Richtsnoeren College Bescherming Persoonsgegevens (CBP)
	Privacy Impact Assessment (PIA)
Handreikingen	Grip op privacy: De Privacy Baseline, definitief, versie 1.0, 30 november 2015; Centrum Informatiebeveiliging en Privacybescherming (CIP)
	Grip op privacy: Handleiding Privacy by Design, concept, 22 februari 2016; Centrum Informatiebeveiliging en Privacybescherming (CIP)
	Grip op Secure Software Development (SSD). Beveiligingseisen voor (web)applicaties, versie 2.0, 5 oktober 2014, Centrum Informatiebeveiliging en Privacybescherming (CIP)

Baseline Informatiebeveiliging Rijksdienst (BIR)
De voor de overheid verplichte standaarden ISO27001/ISO27002 zijn met aanvullingen opgenomen in de BIR. De BIR TNK is voor de Rijksoverheid verplicht. Afwijkingen zijn onder voorwaarden soms mogelijk.

De BIR is een gemeenschappelijke standaard die uitwisseling van departementaal vertrouwelijke informatie binnen de Rijksoverheid vergemakkelijkt door informatiebeveiligingsrisico's controleerbaar te beperken of op te heffen. Een gedeelte van de implementatie van de BIR normen zal door de Applicatie-dienstverlener uitgevoerd moeten worden. De BIR is geen doel op zich maar een norm binnen het Rijk om op uniforme wijze risico's tot acceptabele grootte terug te brengen voor als "Departementaal vertrouwelijke informatie" gerubriceerde informatie.

5. IB Beleid

Het informatiebeveiligingsbeleid is vastgesteld in het document "05 1 1 (r) ~~IBV beleid~~IBV-beleid CIZ [V2.00].pdf". Hieronder volgt een korte samenvatting.

Informatiebeveiliging volgt de eisen vanuit wet en regelgeving en de missie en visie van CIZ om haar taak zo efficiënt en effectief mogelijk uit te voeren. CIZ draagt vanuit haar rol een grote verantwoordelijkheid ten aanzien van het waarborgen van de vertrouwelijkheid van de medische gegevens van al onze cliënten. Door het integraal mee nemen van informatiebeveiliging in de eisen bij de ontwikkeling en implementatie van bedrijfsprocessen en ~~ICT voorzieningen~~ICT-voorzieningen wordt de informatieveiligheid bij vernieuwingen geborgd. Daarnaast worden voor de staande ~~ICT omgeving~~ICT-omgeving en bedrijfsprocessen cyclisch risico analyses uitgevoerd, informatiebeveiligingsrisico's inzichtelijk gemaakt en proportionele mitigerende maatregelen getroffen.

De BIR is binnen de rijksdienst voorgeschreven. Ook CIZ volgt dit beleid en legt hierover verantwoording af aan het ministerie van VWS in de vorm van een In Control Verklaring (ICV). Periodieke interne en externe audits meten de compliance van CIZ aan de BIR.

De maatregelen in de BIR zijn passend voor departementaal vertrouwelijke informatie. Persoonsgegevens in de categorie 2 van de WBP vallen hier ook binnen. Voor bijzondere persoonsgegevens (WBP cat. 3), in het geval van CIZ zijn dat medische gegevens, zijn aanvullende maatregelen nodig.

6. Inrichting van de informatiebeveiliging

De vicevoorzitter van de raad van bestuur is eindverantwoordelijk voor de informatiebeveiliging. Het lijnmanagement is gedelegeerd verantwoordelijk voor de informatiebeveiliging in algemene zin en specifiek voor de BIR normen behorende bij haar verantwoordelijkheidsgebied.

De CIO is door het bestuur gemandateerd voor alle besluiten op tactisch niveau op het gebied van informatiebeveiliging. Samen met de CISO en de internal auditor geeft hij sturing aan de informatiebeveiligingsaspecten binnen de organisatie en rapporteert minimaal een maal per kwartaal aan het bestuur. Tevens wordt er maandelijks een Security Board gehouden waarbij de CISO de voorzitter is van dit overleg.

Vernieuwingen op bedrijfsvoering niveau worden besproken in ~~het Advisory Board of Changes (ABC)~~de Bestuursraad en op ICT niveau in de Change Advisory Board (CAB). Voor beide processen is IB aangehaakt om zorg te dragen dat bij wijzigingen het huidige beveiligingsniveau minimaal gehandhaafd blijft.

Rapportages van de normeigenaren(waaronder incidentrapportages) en uitkomsten van reguliere en ah hoc security audits zorgen voor inzicht in de actuele risico's, de effectiviteit van processen en maatregelen en uiteindelijk het actuele risicoprofiel van het CIZ voor de informatiebeveiliging.

7. CIZ IB strategie en eisen per thema

Bij de onderstaande thema's wordt meer per onderwerp ingezoomd op de informatiebeveiligingsaspecten, eisen en oplossingsrichtingen. Deze komen dus boven op de reeds gestelde kaders.

7.1 Classificatie van informatie

Het CIZ verwerkt naast de gebruikelijke bedrijfsvoering informatie (bestuurlijke-, personele-, financiële informatie, etc.) een grote hoeveelheid bijzondere persoonsgegevens. Het gaat hier om medische informatie afkomstig van cliënten zelf en informatie aangeleverd vanuit de medische disciplines. De omgang met dit type informatie vraagt extra aandacht om de privacy van de

cliënten te kunnen garanderen, maar ook om aan specifieke wettelijke normen te kunnen voldoen (zoals de Archiefwet).

Vertrouwelijkheid
CIZ gebruikt voor de indeling van de vertrouwelijkheid van haar informatie 3 categorieën, nl:

1. *Openbare informatie*
   Dit is alle informatie die CIZ publiekelijk beschikbaar stelt via rapportages, eigen website e.d.

2. *Vertrouwelijke informatie*
   De BIR schrijft maatregelen voor die voldoende zijn voor de beveiliging van informatie tot en met Departementaal Vertrouwelijk. De reguliere ~~CIZ bedrijfsvoeringinformatie~~CIZ-bedrijfsvoeringinformatie valt hier onder en ook de Wbp categorie 2 persoonsgegevens.

3. *Geheime informatie*
   De medische gegevens die CIZ verwerkt vallen onder de Wbp categorie 3. Daarnaast heeft CIZ informatie die bij uitlekken schadelijk kunnen zijn, zoals bijvoorbeeld informatie over fraudeonderzoeken. Deze informatie soorten vragen om een aanvullende maatregelen bovenop die van de BIR om de vertrouwelijkheid te waarborgen.

7.2 Identity Access Management (IAM)

CIZ wil haar organisatie en bedrijfsprocessen slim en efficiënt inrichten zodat de klant optimaal wordt bediend (snelheid, kwaliteit), maar wil ook nadrukkelijk de privacy van de klanten waarborgen. Beschikbaarheid en vertrouwelijkheid zijn twee kanten van dezelfde medaille. De gevolgen van het uitlekken van vertrouwelijke informatie worden door de striktere wetgeving steeds groter en vragen daardoor om aandacht, zorg en controle om die te voorkomen.

Vertrouwelijkheid
Het informatiebeveiligingsbeleid van het CIZ stelt daarom dat medewerkers alleen toegang hebben tot die informatie die noodzakelijk is voor de uitvoering van hun functie of rol. De toegang tot de ~~CIZ werkomgeving~~CIZ-werkomgeving, -systemen en -informatie moet fijnmazig gereguleerd kunnen worden. De authenticatie moet passen bij de wijze van toegang tot, en de classificatie van de informatie en zal moeten voldoen aan de in de BIR gestelde eisen op het gebied van logische toegangsbeveiliging.

Beschikbaarheid
De toegang tot de ~~CIZ werkomgeving~~CIZ-werkomgeving, -systemen en -informatie moet laagdrempelig en gebruikersvriendelijk zijn. Een tijd-, plaats- en apparaat-onafhankelijke standaard digitale werkomgeving die alleen bij het aanmelden om authenticatie vraagt, ook als er vanuit de ~~CIZ werkomgeving~~CIZ-werkomgeving systemen met authenticatie buiten het CIZ domein worden aangeroepen (ASP/SAAS). Management van de autorisaties zoveel mogelijk centraal belegd, maar daar waar flexibiliteit noodzakelijk is voor de bedrijfsvoering kan het uitdelen van rechten in de organisatie belegd worden. Zo zouden managers zelf tijdelijke rechten kunnen toekennen voor de systemen waar zij eigenaar van zijn, in zoverre dit geen onacceptabele risico's met zich mee brengt.

7.3 Access devices, digitale werkomgeving en opslag van CIZ data

Door een gebruikersvriendelijke werkomgeving aan te bieden (door o.m. te letten op aspecten zoals die hierboven zijn genoemd) wordt de behoefte van medewerkers om eigen oplossingen te introduceren verkleind. ~~Echter is c~~Consumerization, zoals BYOD, is echter een voldongen feit en vraagt alertheid en flexibiliteit. Vanuit informatiebeveiligingsoogpunt dienen de volgende principes gehanteerd te worden:

- CIZ heeft zicht op waar haar bedrijfsdata is opgeslagen (device/plaats).
- CIZ heeft controle over deze data (beschikbaarheid, integriteit, vertrouwelijkheid en controleerbaarheid)
- zero footprint voor de devices is het uitgangspunt (zoals in de BIR gesteld).

- de opslag en bewaring van gegevens voldoet aan de continuïteitseisen van CIZ, de archiefwet en wetgeving op het gebied van de privacy.

7.4 Ontwikkeling en onderhoud/beheer informatiesystemen

Bij de ontwikkeling van informatiesystemen moeten samen met de functionele wensen ook de eisen t.a.v. de beveiliging en, indien van toepassing, fraudepreventie worden meegenomen. Het CIZ heeft nog niet formeel de Secure Software Development geadopteerd[1], maar staat positief tegenover deze aanpak en ziet die in samenspraak met haar dan ook graag gebruikt worden bij de ontwikkeling en onderhoud van maatwerkapplicaties. ~~.~~Tevens wordt uitgegaan van het concept Privacy by Design bij het onderhouden en ontwikkelen van Portero en DWH.

Voor ontwikkelomgevingen zijn beperktere eisen ten aanzien van de informatiebeveiliging mogelijk. Daarbij moet dan wel aan een aantal randvoorwaarden worden voldaan, zoals het in eerste instantie volledig ontbreken van bedrijfsvoeringdata in het ontwikkeldomein, een volledig van de rest van het ~~ICT landschap~~ICT-landschap gescheiden zone met strikte protocollen t.a.v. de export van code naar de test en productieomgevingen.

Externe toegang tot de CIZ ICT systemen voor ontwikkel/beheerwerkzaamheden dient op één uniforme wijze te zijn gefaciliteerd, waarbij nooit sprake is van rechtstreekse toegang tot het interne ~~CIZ netwerk~~CIZ-netwerk maar bijvoorbeeld via een stepping stone constructie. Tooling voor beheerwerkzaamheden worden binnen het ~~CIZ domein~~CIZ-domein gehost.

Voor externe toegang tot de ontwikkelomgeving of ten behoeve van beheeractiviteiten is 2 factor authenticatie vereist.

[1] "20140312_Grip-op-SSD-Het-proces-v1-02.pdf"