Bijlage 3 bij de verwerkersovereenkomst
Landelijke Aanpak Adreskwaliteit

Beveiliging

Versie 25 april 2018

De beveiliging van de dataverwerking binnen het Informatie Knooppunt (IKP) van het programma Landelijke Aanpak Adreskwaliteit (de LAA) is op orde. Dit blijkt onder meer uit de rapporten van de diverse audits die op de IKP-omgeving en -processen zijn uitgevoerd.

ICTU verwerkt de persoonsgegevens in het IKP op een technisch gescheiden, beveiligde omgeving die alleen voor dit doel wordt gebruikt. Er zijn verscheidene fysieke, procedurele en technische maatregelen genomen om gegevens in deze omgeving te beschermen en om gecontroleerd gegevens van en naar deze omgeving te brengen:

- **fysieke** maatregelen: alleen toegang tot persoonsgegevens vanuit één afgesloten kamer, afgesloten en gehardende werkstations
- **procedurele** maatregelen: o.m. rolscheiding, toepassing vier-ogen principe, minimale rechten, patchbeleid
- **technische** maatregelen: o.m. netwerkzonering en firewalling, meerdere niveaus van verbindingsbeveiliging (encryptie), twee-factor authenticatie, hardening, auditlogging, malwarescanning

Transport van gegevens vindt plaats via beveiligde verbindingen.
Opslag van gegevens vindt alleen plaats in Overheids Datacentrum Rijswijk en in een beveiligde serverruimte bij ICTU (als off-site backup). Er worden dagelijks backups gemaakt die op twee fysieke beveiligde locaties worden opgeslagen. Opzet en inrichting zijn frequent door onafhankelijke derde partijen getoetst.

Inhoud:

A. Informatiebeveiligingsniveau

ICTU heeft de operationele werkzaamheden van LAA in het IKP beveiligd in overeenstemming met de Tactisch Normenkader Baseline Informatiebeveiliging Rijksdienst (BIR) 2017 op het basisbeveiligingsniveau 2: BBN2.
De BIR2017 onderkent voor de generieke schades en dreigingen voor de Rijksoverheid drie basisbeveiligingsniveaus (BBN's), waarvoor bijbehorende beveiligingseisen gesteld zijn. BBN2 komt overeen met de bescherming die vanuit de Tactische Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG) geboden wordt.

Zowel de BIG als het BIR zijn gestructureerd volgens NEN/ISO 27001, bijlage A en NEN/ISO 27002. De overheid is conform de voorschriften van het College Standaardisatie, verplicht om aan ISO 27001 en ISO 27002 te voldoen middels het principe: pas toe of leg uit.

B. Beveiligingsmaatregelen (7 aspecten)

Het IKP gebruikt twee informatiesystemen waarin persoonsgegevens van burgers worden verwerkt:

1. de webapplicatie LAA (WALAA): een ondersteunende vragenlijstapplicatie die gemeenten gebruiken voor het uitvoeren van adresonderzoeken;
2. een data-analyse omgeving, waarin risicoprofielen worden verwerkt.

Beide informatiesystemen worden in het IKP ontwikkeld, gebruikt en beheerd. De eindgebruikers van de WALAA zijn de gemeenteambtenaren. Voor LAA is een beveiligingsbeleid opgesteld en in werking dat bestaat uit zeven aspecten.

1 Organisatie van informatiebeveiliging LAA
LAA volgt het informatiebeveiligingsbeleid van ICTU, dat door de directie van ICTU is vastgesteld. Dit beleid is een nadere specificering van de Baseline Informatiebeveiliging Rijksdienst (BIR).

Binnen ICTU valt de informatiebeveiliging onder de verantwoordelijkheid van de CISO (Chief Information Security Officer). Aanvullend op dit beleid heeft LAA risico-gebaseerd specifieke aanvullende maatregelen geïmplementeerd. Dit LAA-specifieke beleid valt onder de LAA security officer. De LAA security officer rapporteert aan de programmaleiding LAA en aan de CISO ICTU.

Periodiek en vóór iedere grote wijziging worden op basis van een risicoanalyse de beoogde maatregelen beoordeeld en verfijnd waar nodig. De laatste risicoanalyse is in Q1 2017 uitgevoerd door een externe partij (VKA) voor de implementatie van IKP 2.0. (Beoogde) maatregelen worden vastgelegd in een elektronisch ticketingsysteem en toegewezen aan één verantwoordelijke. Op elk moment is

hiermee de status van de implementatie inzichtelijk (gepland, onder handen, voltooid).

2 Fysieke beveiliging

Dataverwerking gebeurt in een fysiek afgesloten 'IKP-ruimte'. De locatie waarin de IKP-ruimte gelegen is, is alleen toegankelijk voor medewerkers met een geautoriseerde toegangspas. De IKP-ruimte zelf is alleen toegankelijk voor IKP-medewerkers met een eigen elektronische contactloze sleutel. Passanten kunnen niet op de computerbeeldschermen kijken. De servers van het IKP en de webapplicatie van LAA staan in het Overheids Datacenter (ODC) in Rijswijk. Daar is de toegang strikt beveiligd.

De IKP-werkplekken bestaan uit desktops met vaste bekabeling, wat betekent dat dataverwerking alleen in de IKP-ruimte (on site) mogelijk is. De desktops in de IKP-ruimte staan in afgesloten kasten, gemonteerd onder het bureau. Hierdoor wordt het onmogelijk andere randapparatuur aan te sluiten dan wat standaard aangeboden wordt (toetsenbord, muis en monitor). De externe opslag (USB, DVD, SD-kaart, e.d.) en draadloze verbindingsmogelijkheden van de IKP werkstations zijn uitgezet (gehardende werkstations). Hierdoor is het niet mogelijk voor een medewerker om data zonder assistentie op of buiten de IKP-omgeving te brengen (fysiek en technisch afgedwongen vier-ogen principe). Technisch beheer van de webapplicatie van LAA vindt plaats vanaf een speciale laptop, die na gebruik in de kluis op de IKP-ruimte wordt opgeslagen.

3 Medewerkers

Elke LAA-medewerker heeft een relevante VOG en geheimhoudingsverklaring ondertekend. Deze documenten zijn terug te vinden in het dossier van de betreffende medewerker. Om te kunnen werken op de IKP-werkplekken worden strikte autorisatie en identificatie richtlijnen gevolgd. De externe medewerkers hebben alleen via de vaste IKP-werkplek toegang tot de data en dataverwerking. LAA-medewerkers worden actief op de hoogte gebracht van de geldende beveiligingsmaatregelen. Deze maatregelen worden frequent getoetst.

IKP-medewerkers werken volgens gedefinieerde rollen. Iedere medewerker heeft één specifieke rol. Aan rollen zijn bepaalde rechten gekoppeld; deze rechten zijn de minimale waarmee de werkzaamheden efficiënt kunnen worden uitgevoerd. Zo kan een applicatiebeheerder niet in de database, en kunnen databasebeheerders geen applicatie- of systeeminstellingen wijzigen. Gebruiks- en beheerrollen zijn strikt gescheiden.

Elke 3 maanden moeten toegangsrechten van IKP-medewerkers expliciet worden verlengd. Na afloop van de inzet van een medewerker bij het IKP worden de toegangsrechten ingetrokken. Deze maatregelen gelden niet alleen voor de analisten van het IKP, maar ook voor de technisch en applicatie-beheerders die verantwoordelijk zijn voor het operationeel maken en houden van de IKP-informatiesystemen.

4 Procedurele maatregelen

IKP implementeert gangbare procedurele maatregelen om het vereiste niveau van informatiebeveiliging te halen. Deze maatregelen hebben betrekking op het beheer van:

- wijzigingen
- incidenten - uitgewerkte en gecommuniceerde procedure rondom het melden van datalekken
- toegangsbeveiliging - rolscheiding, minimale rechten per rol, toepassing vier-ogen principe
- personeel- (proces in- en uit dienst) en
- continuiteïtsbeheer - backup en restore

5 Technische maatregelen

IKP gebruikt voor de data-analyse een afzonderlijke, logisch en fysiek gescheiden IT-infrastructuur. Deze infrastructuur bestaat uit twee delen:

1. de werkplekken in de IKP-ruimte in het kantoor van ICTU en
2. de servers in het Overheids Datacentrum Rijswijk (ODC Rijswijk).

Beide omgevingen zijn gescheiden van de reguliere IT-omgevingen van ICTU: er is geen toegang mogelijk tot de reguliere ICTU-omgeving vanuit de IKP-omgeving. En omgekeerd is ook geen toegang mogelijk vanaf de ICTU-omgeving naar de IKP-omgeving. Beide omgevingen zijn ook zodanig ingericht dat er géén toegang is vanaf, of naar internet - met uitzondering van het gericht binnen kunnen halen van software-updates. Vanaf de IKP-werkplekken in de IKP-ruimte kan alléén met de IKP-omgeving in ODC Rijswijk gewerkt worden. En omgekeerd kan de IKP-omgeving in ODC Rijswijk alléén gebruikt worden vanaf de IKP-werkplekken in de IKP-ruimte. Ook het technisch beheer is alleen mogelijk vanuit de IKP-ruimte.

Bij de inrichting van de omgevingen is gebruik gemaakt van gangbare beveiligings-maatregelen, zoals firewalling en netwerkzonering, hardening (alleen die hard- en software activeren die daadwerkelijk gebruikt wordt), malwarescanning, gebruik van versleutelde verbindingen (meerdere niveaus), twee-factor authenticatie van gebruikers, disk-encryptie, auditlogging.

De webapplicatie van LAA (WALAA) die gemeenten gebruiken bij de adresonderzoeken is noodzakelijkerwijs wel via Internet toegankelijk. Deze toegang is beperkt op IP-adresbereik (geofencing). LAA is bezig met de gefaseerde overgang naar twee-factor authenticatie van gebruikers van de WALAA op basis van eHerkenning-middelen op betrouwbaarheidsniveau 3 (naar verwachting gelijkwaardig aan betrouwbaarheidsniveau eIDAS Substantieel).

6 Logging

In de analyse en gegevensverwerking worden alle processtappen gelogd. De datakwaliteit controle wordt gelogd naar de database én een bestand. Op de niveaus van bestand, tabel en data is bepaald wie wat mag en kan doen. Op elk moment kan achterhaald worden wie wanneer wat met de data gedaan heeft. Binnen de dataverwerking zijn alle rollen gescheiden:

- medewerkers die de data binnenhalen, kunnen de data niet bewerken
- medewerkers die de data bewerken, kunnen nooit de logging van hun eigen bewerkingen beïnvloeden

Naast deze logging op functioneel niveau is voor de verantwoording ook technische auditlogging geïmplementeerd. Deze log legt op gedetailleerd niveau vast wat op de omgeving gebeurt (wie, wat en wanneer), bijvoorbeeld het in- en uitloggen, opzetten van netwerkverbindingen, kopiëren van bestanden, wijzigen van toegangsrechten, etc. Deze log is niet toegankelijk voor IKP-gebruikers.

7 Gegevensuitwisseling

Elke datalevering tussen een leverancier die overheidspartij is en het IKP, zowel inkomend als uitgaand, wordt vooraf wederzijds getoetst en wordt vastgelegd, bijvoorbeeld in een Gegevens Levering Overeenkomst (GLO) of convenant. Bij elke fundamentele wijziging van de datalevering wordt dit aangepast. De datalevering en wijzigingen daarop worden tevens opgenomen in de verwerkersovereenkomst (VWO) met gemeenten. Middels de VWO is ICTU bevoegd om persoonsgegevens van de betreffende gemeente te verwerken.
In de VWO en vastlegging met dataleveranciers staat ten minste:

- de gegevenslevering en het afgesproken dataformat
- doel van de gegevensverwerking
- juridische grondslag

Gegevensuitwisseling met leveranciers gebeurt in overleg met een beveiligde verbinding. Op dit moment is deze beveiligde verbinding nog niet direct gekoppeld aan de beveiligde omgeving van het IKP. Data die door deze beveiligde verbinding binnenkomen, worden handmatig overgezet op de beveiligde omgeving van het IKP. Een automatische, beveiligde koppeling met het IKP wordt in de toekomst gerealiseerd.

Vanaf de start van het IKP tot op heden wordt de volgende procedure voor gegevensuitwisseling gehanteerd:

Dataleveranciers leveren bestanden aan via de beveiligde verbinding. De bestanden worden opgehaald op één specifieke laptop die alleen voor dit doel wordt gebruikt. Met leveranciers is afgesproken dat zij alleen versleutelde bestanden mogen opsturen. Dat betekent dat de bestanden met een wachtwoord zijn beveiligd. Het wachtwoord wordt separaat verstuurd via een ander medium (sms) naar een andere analist dan degene die de beveiligde link van het bestand heeft ontvangen. Deze procedure zorgt ervoor dat voor lekken van data minimaal twee middelen (laptop en mobiele telefoon) en twee mensen (analist die de link ontvangt en analist die het wachtwoord ontvangt) nodig zijn.

Vervolgens wordt het versleutelde bestand naar de IKP-omgeving overgezet. Dit gebeurt via een beveiligde USB-stick. Deze USB-sticks voldoen aan de Amerikaanse FIPS140-2 norm en zijn door het Nationaal Bureau Verbindingsbeveiliging van de AIVD goedgekeurd voor transport en opslag van gegevens tot en met het niveau VIR-BI Departementaal Vertrouwelijk. Zodra de bestanden op de USB-stick staan, worden ze direct permanent verwijderd van de laptop. De bestanden zijn op dit moment nog steeds versleuteld.

Het bestand wordt vervolgens door twee personen uit twee verschillende rollen vanaf de USB-stick op de beveiligde IKP-omgeving geplaatst. De IKP-omgeving vereist minimaal één persoon met rechten van een data-analist en één persoon met rechten van een beheerder om bestanden over te zetten. Dit is het vier ogen principe dat ook technisch wordt afgedwongen. Bij het overzetten, wordt het bestand tevens gescand op malware.

Het bestand wordt pas na succesvolle verwerking van de USB-stick verwijderd om bij eventuele fouten het bestand niet weer opnieuw te hoeven ophalen. De USB-stick zelf is versleuteld met een wachtwoord dat alleen in een wachtwoordkluis staat. USB-sticks zelf worden altijd in de kluis in de afgesloten IKP-ruimte opgeslagen.

C Resultaten uitgevoerde audits (Analyse omgeving en LAA-applicatie (WALAA))

Analyse omgeving in het IKP: In de periode van 18 november 2015 tot en met 18 december 2015 is een onderzoek naar de *beveiliging van het IKP* uitgevoerd conform de NOREA 3000 richtlijn 'Assurance opdrachten door IT-auditors'. Dit is uitgevoerd door Bureau voor Kwaliteitsborging bij de Overheid (BKBO). Op 1 maart 2016 heeft BKBO haar Assurancerapport ICTU 2015 met kenmerk BKBO/151104/AR opgeleverd met de volgende positieve conclusie:
"Wij (BKBO) zijn van oordeel dat de interne beheersingsmaatregelen met betrekking tot het IKP in alle van materieel belang zijnde opzichten effectief zijn". [..] Daarmee voldoet ICTU LAA/IKP aan de Wet bescherming persoonsgegevens (WBP) en aan de zelf opgelegde norm BIR.

WALAA-omgeving: Het tweede onderzoek betreft de beveiliging rond het gebruik van de LAA-applicatie, die via iPads aan gemeenten ter beschikking wordt gesteld. Hierbij is het van belang dat de LAA met elke deelnemende gemeente een verwerkersovereenkomst (VWO) sluit, alvorens IKP de data levert aan een gemeente. Een gemeente kan altijd alleen die data zien die specifiek voor die gemeente gelden. Een gemeente is zelf verantwoordelijk voor het beheer van de iPads en tevens verantwoordelijk voor het toezien op het juist gebruik van de iPads conform de BIG richtlijnen.

Het onderzoek op de WALAA werd uitgevoerd door [redacted] (ITSX BV), in de maanden voorafgaand aan de publicatie in september 2015. De hoofdconclusie van het rapport was: "De centrale componenten en technische koppelvlakken voor de ontsluiting van de data van de omgeving zijn afdoende beveiligd, mits een laatste technische instelling wordt aangepast. Dit betreft de configuratie van de versleutelde verbindingsinstellingen [..]". Inmiddels is deze configuratie begin 2016 volgens het advies van [redacted] ingeregeld. Het rapport stelt verder o.m. dat: "Op basis van de aanwezigheid van de bewerker overeenkomsten en onderlinge afspraken voldoet de keten aan de wet bescherming persoonsgegevens".

Analyse omgeving in het IKP: In de tijdsperiode van 24 april tot en met 12 mei 2017 heeft de externe derde partij, Deloitte Risk Advisory B.V., een security test uitgevoerd

op de IKP-omgeving die op het ODC in Rijswijk draait. Tijdens de security test is een aantal kwetsbaarheden geïdentificeerd met een middelgroot tot laag risico. Op aanraden van Deloitte zijn deze in het rapport beschreven kwetsbaarheden opgelost voordat het IKP in productie is genomen op het ODC-platform. Bij grotere wijzigingen wordt een nieuwe test uitgevoerd.