Privacy by design

Gemeente Leiden, Leiderdorp, Oegstgeest, Zoeterwoude & Servicepunt71

Versie 1.4

19-7-2016

Versiebeheer

1.1	7 privacy principes toegevoegd, wachtwoordvereiste aangepast
1.2	Kopje optioneel toegevoegd, hier opgenomen wanneer certificering gevraagd moet worden
1.3	Kop 2.2.Realiseren behoefte informatiesysteem aangescherpt op basis van actuele informatie van het Centrum Informatiebeveiliging en privacybescherming (CIP)
1.4	Aanpassen van inleiding en kleine tekstuele zaken nav voorbespreking met voorzitter stuurgroep VRIS.

Inhoud

1. Inleiding

Van overheidsorganisaties wordt op dit moment al verwacht dat zij persoonsgegevens goed beveiligen. In de nabije toekomst worden de eisen rond privacybescherming nog strikter. Zo geldt sinds 25 mei 2016 de Algemene Verordening Gegevensbescherming (AVG). Alle organisaties in de publieke en private sector worden geacht om vanaf die datum hun bedrijfsvoering met de AVG in overeenstemming te brengen en krijgen hiervoor tot 25 mei 2018 de tijd. De AVG vervangt op dat moment direct de huidige Wet bescherming persoonsgegevens (Wbp).
Een van de aspecten uit de AVG is dat een organisatie op het gebied van privacybescherming accountable en auditable[1] zijn. Dit neemt een documentatieplicht met zich mee.

Om aan aspecten van de AVG te kunnen voldoen is het document Privacy by design opgesteld. Privacy by design houdt in dat wij als organisatie al tijdens de ontwikkeling van producten en diensten (zoals informatiesystemen) aandacht besteden aan het volgende:

1. Privacy verhogende maatregelen, ook wel privacy enhancing technologies (PET) genoemd.
2. Dataminimalisatie. Dit houdt in dat er zo min mogelijk persoonsgegevens verwerkt worden, of te wel alleen de gegevens die noodzakelijk zijn voor het doel van de verwerking.

Op deze manier kan een zorgvuldige en verantwoorde omgang met persoonsgegevens technisch worden afgedwongen.

Om dit te kunnen borgen hanteren we de volgende 7 principes:

1. Privacy als standaard
2. Proactief in plaats van reactief
3. Preventief in plaats van herstellend
4. Privacy is aantoonbaar, het is geïntegreerd in het ontwerp en aanwezig in alle functionaliteiten
5. Privacy van het begin tot het eind, beschermt en ondersteund tijdens de volledige levenscyclus
6. Privacy is zichtbaar en transparant, onze inwoners weten hoe we met hun gegevens omgaan
7. Respect voor privacy

Dit document bevat richtlijnen waaraan een informatiesysteem die persoonsgegevens verwerkt moet voldoen om deze persoonsgegevens te beschermen. Deze richtlijnen gelden voor nieuwe een bestaande informatiesystemen. Het is een maatregel die afkomstig is uit het Beleid Gegevensbescherming - Privacy en veiligheid verwerking persoonsgegevens gemeente Leiden, Leiderdorp, Oegstgeest & Zoeterwoude. Deze maatregel heeft ook een nauwe relatie met het Informatiebeveiligingsbeleid.

2. Privacy by design

Privacy by design is niet alleen een checklist die alleen bij de aanschaf of implementatie van een informatiesysteem doorlopen moet worden. Ook wanneer een informatiesysteem operationeel is, zal regelmatig getoetst moeten worden of er voldaan wordt aan de Wet bescherming persoonsgegevens. Dit wordt uitgevoerd door de Functionaris Gegevensbescherming en/of privacy beheerder.

[1] accountable wil zeggen dat er voor privacybescherming in je organisatie en interne controle maatregelen en mechanismen zijn ingebouwd. Auditable wil zeggen dat je die maatregelen en mechanismen kan aantonen en dat je kan bewijzen dat ze effectief werken.

2.1. Inventariseren behoefte informatiesysteem

Het kan zijn dat er een behoefte is aan een nieuw of een grote wijziging[2] in een informatiesysteem. Wanneer dit het geval is, is het noodzakelijk dat er voordat over wordt gegaan aan de invulling van de behoefte er een aantal analyses worden uitgevoerd:

- Baselinetoets (inclusief schema gegevensstromen / gegevensproces)
- Privacy impact analyse
- Dataclassificatie
- Diepgaande risico analyse (afhankelijk van de uitkomst van de Baselinetoets)

Deze analyses geven inzicht aan welke beveiligingseisen er moet worden voldaan.

2.2. Realiseren behoefte informatiesysteem

Wanneer er een inventarisatie is gedaan, kan overgegaan worden naar het realiseren van de behoefte tot een nieuw informatiesysteem of het doorvoeren van een grote wijziging.
Om ervoor te zorgen dat de privacy van persoonsgegevens geborgd blijft zullen er als onderdeel van het contract de volgende documenten moeten worden opgesteld:

- Minimaal inkoopvoorwaarden ARBIT-2014
- Bewerkersovereenkomst

Ook moet getoetst worden of het nieuwe informatiesysteem of de wijziging voldoet aan de standaarden zoals die door de Gemeentelijke Model Architectuur (GEMMA) zijn voorgeschreven.

Daarnaast zijn er ook een aantal technische en organisatorische eisen waaraan moet worden voldaan. Betrek wanneer nodig de CISO, privacy beheerder of de FG bij het vastleggen van de eisen in het contract of de bewerkersovereenkomst.

- Technische eisen algemeen
    - Het informatiesysteem moet foutloos kunnen functioneren binnen een SBC (Server Based Computing via Hyper-V ; Xenapp) omgeving, met applicatie virtualisatie (App-V) zoals deze in gebruik is binnen de Leidse regio gemeenten.
    - De gegevensstromen van het informatiesysteem moeten ter beschikking worden gesteld, ook na het uitbrengen van releases.
- Beveiliging
    - De leverancier moet minimaal ISO27001 (Informatiebeveiliging) certificering hebben en kunnen tonen.
    - Leverancier kan een recent auditrapport overleggen.
    - Het informatiesysteem moet wanneer relevant versleuteld communiceren (bijv. over SSL).
    - Bij een cloudoplossing of informatiesysteem die voor meerdere doeleinden wordt gebruikt moeten de gegevens gescheiden van elkaar worden opgeslagen en worden afgeschermd.
    - Persoonsgegeven moet versleuteld worden opgeslagen in de database.
    - Op de opslag van gegevens wordt een datamodel gehanteerd. Binnen het datamodel wordt in de opslag van gegevens verfijning[3] gehanteerd op basis van gegevensgroepen. Gegevensgroepen worden gevormd op basis van de samenhang in functionele zin en qua doelbinding.
    - Bij uitwisseling van informatie tussen informatiesystemen mogen niet-geautoriseerde geen toegang hebben tot de data.

[2] een wijziging die een grote impact heeft op de werking van het informatiesysteem
[3] granulariteit

    - Het informatiesysteem biedt de mogelijkheid ongeautoriseerde toegang te rapporteren middels een email / notificatiesysteem.
    - De leverancier gebruikt rekencentra welke zich binnen het gebied van de EER bevinden, alsmede de moederbedrijven, en partners welke eventueel als sub contractor worden ingeschakeld.
    - Het informatiesysteem ondersteunt de beleidsregels omtrent het gebruik van sterke wachtwoorden, wachtwoordverval periode en time-out.
    - Gebruikers moeten geautoriseerd kunnen worden op basis van het need-to-know principe.
    - Bij het werken met casusmanagers of zaakbehandelaars is het breaking glass principe mogelijk. Wanneer een andere gebruiker toegang nodig heeft tot de gegevens, ontvangt deze een melding en moet vermelden waarvoor de toegang noodzakelijk is. Hiervan wordt logging aangemaakt.
- Kwaliteitstandaarden
    - Het informatiesysteem moet bij storingen alle, geaccepteerde en opgeslagen, mutaties bewaren.
    - De verzameling van gegevens kan zo worden ingericht dat er wordt voldaan aan het proportionaliteit- en subsidiariteitsbeginsel.
    - De kwaliteit van de gegevens moet kunnen worden gecontroleerd en wanneer nodig gecorrigeerd.
    - De leverancier moet garanderen dat, bij het gebruik van software van derden, deze software actueel is en ondersteund wordt door de betreffende leverancier. (hulp programma's ; etc).
    - De gemeente en Servicepunt71 behoudt zich het recht voor om, max. 2x per jaar, op haar kosten door een externe partij of eigen inzet, een algehele of gedeeltelijke technische controle te (laten) uitvoeren op basis van wet- en regelgeving en dit aanbestedingsdocument. De leverancier is verplicht hier kosteloos aan mee te werken. Een controle wordt minimaal 2 weken voorafgaand aangekondigd bij de leverancier.
    - Het informatiesysteem doorstaat zo'n technische controle. Bij het niet doorstaan garandeert de inschrijver dat hij alle punten oplost die uit de audit zijn gekomen binnen een vooraf gezamenlijk afgesproken periode.
    - Het informatiesysteem moet een error log bijhouden van fouten. Systeemmeldingen die eindgebruikers krijgen, zijn begrijpbaar.
    - De leverancier moet een ISO9001 certificering hebben en deze kunnen tonen.
- Technisch en functioneel beheer
    - Het informatiesysteem moet alle verwerkingen (structureel en incidenteel) loggen van alle gebruikers en koppelingen (auditing).
    - Iedere verwerking (structureel en incidenteel) dient terug te leiden tot een natuurlijk persoon (de persoon die de verwerking heeft uitgevoerd).
    - Deze logging moet kunnen worden gepresenteerd en ontsloten zodat wij kunnen voldoen aan het inzagerecht. Hierbij moeten wij de presentatie van de gegevens kunnen passen aan de informatievraag van de betrokkene.
    - Voor zover bij koppelingen of gegevensuitwisseling gebruik wordt gemaakt van standaardpoorten, kan de functioneel beheerder bepalen afwijkende poortconfiguraties te gebruiken.
    - Gegevensuitwisseling vindt plaats op basis van het daarbij horende standaard uitwisselingsformaat.
    - Wanneer er een nieuw standaard uitwisselingsformat wordt uitgegeven, zorgt de leverancier dat dit binnen een jaar operationeel is. Is dit niet het geval dan zal er een boete opgelegd worden.

    - De gegevens blijven eigendom van de gemeente. Bij beëindiging van de overeenkomst of bij faillissement werkt leverancier mee aan het overdragen van alle gegevens welke namens de gemeente bij hem zijn opgeslagen.
    - Om te kunnen voldoen aan de archiefwet en het verwijderingsrecht, moet het mogelijk zijn dat persoonsgegevens/dossiergegevens kunnen worden verwijderd uit het informatiesysteem.
      Wanneer er persoonsgegevens/dossiergegevens worden verwijderd, moet dit worden gelogd.
- Releases
    - De leverancier garandeert dat alle instellingen en wijzigingen binnen het informatiesysteem die door de eindgebruiker zelf kunnen worden gedaan, niet overschreven (kunnen) worden bij de implementatie van nieuwe releases (patches, bug fixes, etc). Bij wijzigingen in de structuur van de applicatie waardoor bovenstaande niet mogelijk is, levert de leverancier hiervoor aparte tooling om deze instellingen afzonderlijk te exporteren en na de update weer te importeren.
    - De aanpassingen van het informatiesysteem aan de geldende en toekomstige wet- en regelgeving zijn de verantwoordelijkheid van de leverancier en moeten op de ingangsdatum van de nieuwe wet- en regelgeving zijn doorgevoerd. Tevens moet de leverancier de gemeente hierover informeren.

2.3. Optionele certificering

Een van de vaste eisen is dat een leverancier minimaal ISO27001 certificeren en ISO9001 moet kunnen tonen. In sommige situaties is het nodig om aanvullende certificering te eisen. Dit is afhankelijk van de aard van het proces en/of de gegevens die verwerkt worden.
Of er aanvullende certificering geëist moet worden, wordt aangetoond door dataclassificatie.