Informatie beveiligingsverklaring

GIR

Deze beveiligingsverklaring is opgesteld door Carthago ICT op verzoek van A&O fonds Gemeenten

Versie 1.3 2021

A&O fonds Gemeenten

Duizenden gebruikers vertrouwen hun incidentgegevens toe aan Gemeentelijk Incidenten Rregistratiesysteem (GIR), wij realiseren ons ten zeerste dat dit privacy gevoelige gegevens betreft en geven prioriteit aan de veiligheid van deze gegevens. Wij streven ernaar om ervoor te zorgen dat gebruikersgegevens veilig worden bewaard en dat we uitsluitend de persoonlijke gegevens verzamelen die nodig zijn om op een efficiënte en effectieve wijze onze diensten aan gebruikers te kunnen leveren.

GIR heeft de mogelijkheid om dadergegevens te registreren in de vorm van een naam en geboortedatum. Tevens biedt het de mogelijkheid om zaak-gegevens vast te leggen. De combinatie van zaakgegevens en maatregelen zorgt ervoor dat er sprake is van bijzonder privacy gevoelige gegevens. Hierdoor zijn er aanvullende beveiligingsmaatregelen noodzakelijk. We zullen in deze beveiligingsverklaring expliciet aangeven welke aanvullende beveiligingsmaatregelen genomen zijn.

Deze beveiligingsverklaring is erop gericht om duidelijkheid te geven over de maatregelen die zijn genomen in het kader van beveiliging. Als kader worden gebruikt de AVG (Algemene Verordening Gegevensbescherming, die vanaf 25 mei 2018 de Wbp (Wet bescherming persoonsgegevens) vervangt, BIO (Baseline Informatie-beveiliging Overheid), BIR (Baseline Informatiebeveiliging Rijksdienst) en de SSD (Secure Software Development) norm van het CIP (Centrum Informatiebeveiliging en Privacybescherming).

Jaarlijks beoordelen de eigenaren en de vertegenwoordigers van de gebruikers de beveiligingsmaatregelen en samen met Carthago ICT worden, indien nodig, nieuwe maatregelen genomen.

GIR maakt gebruik van enkele van de meest geavanceerde technologieën voor internetbeveiliging die momenteel op de markt zijn:

Beveiliging van toepassingen en gebruikers

- **SSL/TLS-encryptie:** Alle communicatie met GIR wordt via TLS-verbindingen verzonden. TLS-technologie (Transport Layer Security – de opvolger van SSL-technologie) beschermt communicatie met behulp van zowel serververificatie als gegevensencryptie. Dit zorgt ervoor dat de verzending van gebruikersgegevens veilig is en alleen beschikbaar voor beoogde ontvangers. SSL is verouderd en is uitgeschakeld.
- **Rol gebaseerde autorisatie tot functionaliteit:** Op basis van persoonlijk toegekende rollen krijgen de gebruikers toegang tot specifieke delen van het systeem.
- **Fijnmazige autorisatie met betrekking tot toegang tot gegevens:** Een gebruiker krijgt alleen toegang tot zijn/haar eigen incidenten, incidenten die hij/zij moet afhandelen en incidenten waarop hij/zij toezicht moet houden.
- **Gebruikerswachtwoorden:** Wachtwoorden voor GIR moeten aan de gangbare minimale complexiteits-eisen voldoen. (Minimaal 8 karakters lang, Minimaal 1 cijfer, Minimaal 1 hoofdletter, minimaal 1 niet-alfanumeriek teken)
- **Gegevenscodering:** Alle gegevens worden door de database versleuteld opgeslagen.

Fysieke beveiliging

- **Datacenter/Hosting:** GIR wordt gehost door Previder. Previder garandeert de beschikbaarheid, veiligheid en integriteit van data. Daarnaast neemt Previder duurzaamheid zeer serieus en neemt ze haar verantwoordelijkheid door zitting te nemen in overkoepelende brancheverenigingen. De volgende certificeringen liggen aan dit streven ten grondslag:
  - NEN7510. Sinds 2013 is Previder NEN7510 gecertificeerd.
  - Previder is ISO 9001, 14001 en 27001:2013 gecertificeerd. Door het inrichten van een information security management systeem (ISMS) volgens ISO 27001:2013, wordt de beschikbaarheid, integriteit en vertrouwelijkheid gewaarborgd van informatie en systemen die klanten onderbrengen bij Previder.
  - Previder is ISO 27017 en ISO 27018 gecertificeerd. Dit zijn uitbreidingen op de ISO 27001 norm voor beveiliging van informatie in cloudomgevingen (27017) en specifiek voor de beveiliging van persoonsgegevens (271018).
  - BREEAM "excellent". Volgens BREEAM heeft Previder het eerste datacenter in de wereld dat het predicaat BREEAM "excellent" mag dragen.
  - DigiD Assurance. De clouddiensten van Previder voldoen aan de door de overheid gestelde beveiligingseisen aan DigiD applicatie-omgevingen.
  - Jaarlijks controleert Carthago ICT dat Previder nog over deze certificaten beschikt en dat het toepassingsgebied relevant is.
- **Beveiliging van datacenters:** De datacenters van Previder zijn 24 uur per dag en 7 dagen per week bemand en worden continu bewaakt. De toegang wordt beveiligd via bewakers, bezoekerslogboeken en toegangsvereisten zoals toegangspasjes en biometrische herkenning.
- **Omgevingsbeheersing:** In de datacenters worden temperatuur en luchtvochtigheid geregeld en wordt continu gecontroleerd op afwijkingen. Er zijn rook- en branddetectie- en responssystemen geïnstalleerd.
- **Locatie:** Alle gegevens (inclusief backups) zijn opgeslagen op servers die zich gegarandeerd in Nederland bevinden. Hierdoor hoeft er niet aan aanvullende eisen op het gebied van doorgifte van persoonsgegevens naar landen buiten de EER te worden voldaan.

Beschikbaarheid

- **Connectiviteit:** Volledig redundante IP-netwerkverbindingen met meerdere onafhankelijke aansluitingen.
- **Stroomvoorziening:** Servers beschikken over redundante interne en externe voedingen. De datacenters hebben back-upvoedingen en zijn in staat om stroom te betrekken van de verschillende substations in het net, verschillende dieselgeneratoren en reservebatterijen.
- **Uptime:** De beschikbaarheid van de GIR server wordt voortdurend bewaakt, met onmiddellijke escalatie bij eventuele uitvaltijd.

Netwerkbeveiliging

- **Uptime:** De beschikbaarheid van de netwerkverbinding wordt voortdurend bewaakt, met onmiddellijke escalatie bij eventuele uitvaltijd.
- **Patching:** De allernieuwste beveiligingspatches worden toegepast op alle besturingssysteem- en toepassingsbestanden om nieuw ontdekte kwetsbaarheden te verhelpen.
- **Logboekregistratie en controle:** Centrale registratiesystemen leggen de toegang tot alle interne systemen, met inbegrip van eventuele mislukte verificatiepogingen, vast en archiveren deze.
- **Back-upfrequentie:** Van de database van GIR wordt dagelijks een back-up gemaakt, en dagelijks verspreid naar een gecentraliseerd back-upsysteem voor opslag op meerdere, geografisch verspreide locaties in Nederland.

Organisatorische en administratieve beveiliging

- **Informatiebeveiligingsbeleid:** Carthago ICT is ISO 27001 gecertificeerd.
- **Screening van werknemers:** Alle Carthago ICT medewerkers met toegangsrechten tot de GIR applicatie beschikken over een Verklaring Omtrent het Gedrag (VOG) die maximaal twee jaar oud is.
- **Toegang:** De toegang tot de GIR server is beveiligd met een IP check. Alleen vanuit het netwerk van Carthago ICT kan de server benaderd worden.
- **Auditlogs:** Wij onderhouden een auditlog over GIR. Alle aanpassingen in het systeem worden gelogd en zijn daardoor naspeurbaar. Daarnaast worden alle raadplegingen van bijzonder privacy gevoelige gegevens gelogd waardoor deze handelingen naspeurbaar zijn.
- **Need to know:** Alleen de medewerkers van Carthago ICT die GIR beheren hebben toegang tot de GIR server.
- **Eigen rol gebruikersorganisatie:** Iedere gebruikersorganisatie moet zelf regelmatig valideren dat de juiste rollen aan de juiste medewerkers zijn uitgedeeld. Daarnaast moet de gebruikersorganisatie er zelf op toezien dat het systeem op de juiste wijze ingezet en gebruikt wordt.
- **Termijnen:** Per gebruikersorganisatie kunnen in GIR raadpleegtermijnen gedefinieerd worden. De initiële standaard hiervoor is 24 maanden; dit is ook de maximale raadpleegtermijn. Hierdoor zijn dader-maatregelen zoals bijvoorbeeld pandverboden na maximaal 24 maanden niet meer raadpleegbaar.
- **Schonen:** Informatie in GIR heeft een beperkte bewaartermijn. Na 60 maanden worden de incidenten gearchiveerd. Dit betekent dat dader en slachtoffergegevens van het incident verwijderd worden. Het incident wordt geanonimiseerd, maar kan nog wel in de rapportages en tellingen gebruikt worden. Gebruikersaccounts worden na 36 maanden inactiviteit verwijderd.

Softwareontwikkeling

- **Secure Programming:** Alle Carthago ontwikkelaars zijn speciaal opgeleid voor Secure Programming. Bij het ontwerp van nieuwe functionaliteit worden actief de consequenties en mogelijkheden van informatiebeveiliging afgewogen.
- **Code Review:** Alle aangepaste en nieuwe code wordt door een tweede ontwikkelaar geauditeerd op fouten en security risico's.
- **SSD richtlijnen:** GIR is getoetst aan de Secure Software Development richtlijnen van het Centrum Informatiebeveiliging en Privacybescherming (CIP). De bevindingen uit de toets zijn verwerkt zodat GIR voldoet aan de richtlijnen.
- **Aanpassing ontwikkelproces:** Bij het uitwerken van nieuwe functionaliteit stellen we zogeheten abuse stories op, waarin we analyseren of en hoe de nieuwe functionaliteit misbruikt zou kunnen worden.

Licentieovereenkomst / Verwerkersovereenkomsten

- **Licentieovereenkomst gemeente – A+O fonds Gemeenten**. Het A+O fonds Gemeenten sluit een licentieovereenkomst af met iedere gemeenten die het GIR gebruikt. In deze overeenkomst wordt verwezen naar de eerder genoemde verwerkersovereenkomsten.
- **Verwerkersovereenkomst Carthago ICT – Gemeenten af te sluiten door A+O fonds Gemeenten.** Carthago ICT heeft A+O fonds gemeenten een volmacht gegeven om namens Carthago ICT de in samenwerking met A+O fonds gemeenten vastgestelde standaard verwerkersovereenkomst tussen Carthago ICT en de gemeente af te sluiten. Hierin de is de meldplicht bij datalekken opgenomen.
- **Verwerkersovereenkomst Carthago ICT – Previder.** Carthago ICT heeft met Previder een verwerkersovereenkomst afgesloten. Hierin ook is de meldplicht bij datalekken opgenomen. Deze verwerkersovereenkomst tussen Carthago ICT en Previder is compliant aan de AVG wetgeving en de bovenliggende verwerkersovereenkomst tussen Carthago ICT en Gemeente.

Informatiebeveiliging audits

- Jaarlijks vindt er minimaal één interne security audit plaats door Carthago ICT en een externe security audit door een onafhankelijk auditbureau.
- Gebruikersorganisaties kunnen op eigen kosten aanvullende security audits en/of PEN tests laten uitvoeren. Carthago ICT zal hieraan meewerken tenzij er recent een gelijkwaardige audit of test heeft plaatsgevonden. Voorwaarde is dat de resultaten van de aanvullende audits en tests gedeeld worden met de eigenaren en Carthago ICT.

Fluwelen Burgwal 58
Postbus 11560
2502 AN Den Haag
070 763 00 30
www.aeno.nl

Oktober 2021

A&O fonds Gemeenten