ÉÉN ROTTE APPEL IN DE MAND, MAAKT AL HET GAVE FRUIT TE SCHAND

PRIVACYPROTOCOL

BESCHERMING VAN GEGEVENS

P&O Gevangenenzorg Nederland

Gevangenenzorg Nederland

geloof in herstel

Privacyprotocol

Aanleiding
De doorontwikkeling op het gebied van beveiliging van gegevens noopt Gevangenenzorg Nederland (hierna: GNd) tot het opstellen van dit specifieke protocol voor haar (vrijwillige) medewerkers.

Algemene informatie
Handboek vrijwilligers
In het Handboek vrijwilligers, waarin ook de medewerkers van GNd worden aangesproken, wordt er in artikel 6.3.3. 'Geheimhouding' en in Bijlage 3 'Vrijwilliger en privacy' al nadrukkelijk ingegaan op de rechten en plichten ten aanzien van geheimhouding en privacy.
Nadrukkelijk willen we hier nogmaals stellen dat het van groot belang is dat er geen/zo min mogelijk gegevens die met GNd te maken hebben op (privé-)gegevensdragers (vb. lokale pc, laptop, usb-stick, cd, enz.) opgeslagen worden.

Portal
Vrijwilligers en medewerkers kunnen inloggen op de portal om hun rapportages te maken. Na 40 minuten wordt de gebruiker automatisch uitgelogd. Het beheer van de accounts van vrijwilligers is belegd bij GNd en gebeurt via de interface van CRM. Er wordt op de portal geen geschiedenis bewaard. Mocht een gebruiker / vrijwilliger gehackt worden, dan kan hooguit alleen met diens gegevens worden ingelogd en via doorklikken (in eerste schermen zijn alleen initialen van hulpvrager te zien) de gegevens van diens hulpvrager ingezien worden. Op dat moment is er sprake van inbreuk op de privacy, maar niet van een datalek.

Server
De server is in beheer bij IC-Automatisering. Deze versleutelt gegevens via end-to-end-encryptie, waardoor deze voor hackers niet te lezen zijn. Een mogelijk beveiligingsrisico zou zijn dat de privé pc van een medewerker overgenomen wordt en via de link naar de server daar ingelogd kan worden op het account van de medewerker – daarvoor dienen dan ook de inloggegevens van de gebruiker gestolen te zijn of op automatisch herkennen te staan. GNd heeft dit mogelijk beveiligingsrisico ondervangen door 2 Factor Authenticatie. Deze vraagt naast gebruikersnaam en wachtwoord een extra toegangscode die via een App of SMS naar de gebruiker wordt verzonden. Deze beveiliging is van toepassing op zowel Remote Desktop Server als Webmail.

Datalek
Verlies of diefstal van gegevensdragers of inbraak middels een hack
In een aantal gevallen kan het noodzakelijk zijn om toch gegevens lokaal op een gegevensdrager op te slaan. Doe dit dan altijd gecodeerd met een wachtwoord.
Mocht u onverhoopt geconfronteerd worden met verlies of diefstal van deze gegevensdrager(s), dan dient u onmiddellijk de volgende stappen te doorlopen:
- U meldt dit bij Gevangenenzorg Nederland;
- U meldt het verlies bij de Gemeente waar u iets bent verloren;
- U meldt verlies (als er gevaar voor anderen is) of diefstal bij de politie 0900-8844

Incidentmanagementprocedure
Zodra GNd een melding binnen krijgt van een beveiligingsincident wordt de incidentmanagementprocedure in werking gezet.

Hierbij worden de volgende stappen ondernomen:
1. Melding bij directiesecretaris en/of officemanager via 079-3310568 of info@gevangenenzorg.nl
2. Nagaan wat er vermist of gestolen is.
3. Nagaan welke gegevens hierop stonden van Gevangenenzorg Nederland
4. Intern GNd: de stappen uit het protocol datalekken volgen

170913 Protocol meldplicht datalekk