

Overzicht Datalekken 2016

Naam	Impact	Datum incident	Impact op	Beschrijving	Persoons-gegevens	Gemeld bij AP?	Informereren betrokkenen	Maatregelen
Verzend-fout bij veilig versturen gegevens via mSafe tool bij regionale Back-Office Houten.	Laag	10-3-2016	1.500 kinderen en ouders die jeugdzorg krijgen.	Document met gegevens over 5.500 kinderen i.p.v. gevraagde subset door zorgleverancier, gedeeld via mSafe. Is direct gemeld door zorg-leverancier, document is direct verwijderd bij zorgleverancier en uit mSafe.	Naam, geboortedatum, BSN-nummer, zorgproduct en zorgaanbieder.	JA	Nee, document is via veilig transport in mSafe gegaan, toegang werd gelogd en document is nooit buiten professionele sfeer beland.	Alerter zijn bij regionale Back-Office op gegeven opdracht, want gevraagd werd om cliënten van een zorgleve-rancier die per ongeluk gegevens van alle cliënten in de regio kreeg en controle dat opdracht conform vraag is opgeleverd.
Bij Geynwijs gestolen laptop.	Medium	14-9-2016	125 cliënten van Geynwijs die zorgproducten vanuit de Wmo krijgen, mogelijk risico op identiteits-fraude. Cliënten zijn daarover ingelicht en kregen handleiding.	Uit een woning van een zorgprofessional gestolen laptop bevatte lokale opslag van e-mail.	NAW gegevens, telefoonnummer, e-mailadressen, financiële gegevens, BSN, paspoortkopieën of kopieën van andere legitimatie-bewijzen, geslacht, geboortedatum en/of leeftijd, zorgvragen en -behoefes.	JA	Ja, betrok-kenen kregen een persoonlijke brief met daarin indicatie van de van hen gelekte gegevens.	ICT omgeving (laptops, software) is daarna ingrijpend verbeterd en beveiligd om ervoor te zorgen dat bij een nieuwe diefstal het onmogelijk wordt om toegang te krijgen tot een laptop en dat alle gevoelige data niet meer lokaal staat op de laptop.
Hack bij Provada vastgoed-beurs.	Laag	13-10-2016	1 gebruiker van gemeente op de website van Provada, waarbij inlognaam en wachtwoord werden gestolen.	Informatiebe-veiligingsdienst (IBD) waarschuwde dat vastgoedbeurs Provada was gehackt en dat gegevens van gemeentes op Pastebin stonden.	NAW gegevens, e-mailadres, gebruikersnaam, wachtwoord en telefoonnummers van gebruiker.	Nee	Gebruiker kwam zelf melden met waarschuwingsmail van IBD.	Geen, opvolging lag bij Provada. Wel advies om gebruikt wachtwoord Provada niet ergens anders te gebruiken.

Naam	Impact	Datum incident	Impact op	Beschrijving	Persoonsgegevens	Gemeld bij AP?	Informereren betrokkenen	Maatregelen
Ransomware virus bij Werk en Inkomen Lekstroom (WIL)	Hoog	20-10-2016	18.000 regio cliënten van Werk en Inkomen Lekstroom (WIL) en/of bedrijven werden geëkt door besmetting pc's met virus	Bij WIL is Ransomware binnen-gekomen en heeft alle systemen besmet. Hierbij werd dossierinfor-matie gelekt alsmede de e-mail database.	E-mailadressen uit het adresboek van medewerker. Mogelijk ook persoonlijke gegevens: BSN, NAW, geboortedatum, telefoonnummer en bankrekening-nummer van 18.000 mensen of	JA	WIL heeft alle betrokkenen per brief geïnformeerd namens de bij WIL aangesloten gemeentes.	Aangescherpte ICT beveiliging en awareness instructies personeel WIL m.b.t. gevaar van links naar malafide websites in e-mail.
Fout in adressering bij veilig versturen gegevens via mSafe tool bij regionale Back-Office (RBL) in Houten	Laag	2-11-2016	1 aanvrager PGB	Medewerker van de RBL zette afwijzing op PGB aanvraag die bedoeld was voor Geynwijs in de beveiligde werkruimte van de gemeente IJsselstein. Dit is opgemerkt door een medewerker van de gemeente IJsselstein waarna het bestand is verwijderd uit de werkruimte van IJsselstein en alsnog in de juiste werkruimte van Geynwijs is geplaatst.	NAW en indicatie PGB	JA	Nee, info is nooit buiten beveiligde omgeving mSafe geweest en nooit buiten de sfeer van betrokken professionals.	Geen, was éénmalige vergissing.