NOSUCH

Versie 1 – 01 May 2018

PROTOCOL DATALEKKEN NOSUCH

Opgesteld op:	1 mei 2018
Contactgegevens:	Schiehavenkade 214-222
	3024 EZ ROTTERDAM
	0031 10 2441044
	www.nosuch.nl
	privacy@nosuch.nl

NOSUCH PROTOCOL DATALEKKEN

Dit protocol datalekken wordt geleverd als bijlage van de privacyverklaring en de verwerkersovereenkomsten van NoSuchCompany B.V., hierna te noemen NOSUCH.

INHOUDSOPGAVE

ARTIKEL 1 DEFINITIE DATALEK

Er is sprake van een datalek indien er een inbreuk op persoonsgegevens heeft plaatsgevonden. Een dreiging of tekortkoming in de beveiliging is geen datalek; er moeten daadwerkelijk persoonsgegevens gelekt zijn.

Onder een datalek verstaat de AP persoonsgegevens die gelekt of vernietigd zijn als gevolg van een beveiligingsincident. Bij het lek zijn persoonsgegevens blootgesteld aan verlies of onrechtmatige verwerking. Bij verlies zijn de persoonsgegevens er niet meer. Onder onrechtmatige verwerking vallen bijvoorbeeld onbevoegde kennisneming, wijziging, aantasting of de verstrekking daarvan.

ARTIKEL 2 CONTACTPERSOON

Opdrachtgever en data processor wijzen een contactpersoon aan bij wie eventuele datalekken gemeld moeten worden. Dit kan bijvoorbeeld een bestuurslid of de Functionaris Gegevensbescherming zijn (hierna: 'Contactpersoon' of 'Contactpersonen').

ARTIKEL 3 INFORMEREN MEDEWERKERS

Medewerkers binnen de organisatie dienen zich er van bewust te zijn dat als er sprake is van een datalek, zij dit datalek direct (diezelfde dag nog) moeten melden bij de Contactpersoon, zodat deze tijdig het datalek kan melden bij de AP. Zij dienen bekend te zijn met het in dit protocol opgenomen Stappenplan (ARTIKEL 4).

ARTIKEL 4 STAPPENPLAN

Processtappen	Activiteit	Verantwoordelijk functionaris
1. Er wordt een (mogelijk) datalek ontdekt	- Maak direct intern melding van (het vermoeden van) het datalek - Informeer Contactperso(o)n(en)	Medewerker die het datalek ontdekt
2. Beoordeel het datalek	- Onderzoek het beveiligingsincident - Onderzoek of er persoonsgegevens verloren zijn gegaan of onrechtmatig gebruikt kunnen worden - Beoordeel wie of welke afdelingen binnen de organisatie hierbij betrokken zijn	Manager van de inhoudelijk betrokken afdeling Manager van de afdeling die verantwoordelijk is voor beveiligingsincidenten (bijvoorbeeld: ICT) Contactperso(o)n(en)
3. Bestrijd het datalek	- Stop het datalek als het nog kan - Neem andere maatregelen om het datalek en de gevolgschade te beperken - Documenteer de ondernomen acties	Manager van de inhoudelijk betrokken afdeling Manager van de afdeling die verantwoordelijk is voor beveiligingsincidenten (bijvoorbeeld: ICT) Contactperso(o)n(en)
4.Vaststellen impact	- Onderzoek het datalek en de gevolgen - Onderzoek de aard van de gegevens die gelekt zijn. Bijvoorbeeld: gezondheidsgegevens, wachtwoorden, gegevens over financiële situatie of gegevens die kunnen leiden tot stigmatisering/misbruik - Onderzoek de omvang van de gelekte gegevens - Beoordeel welke impact het lek kan hebben op data subject(s) - Stel vast wat de nadelige gevolgen kunnen zijn	Manager van de inhoudelijk betrokken afdeling Manager van de afdeling die verantwoordelijk is voor beveiligingsincidenten (bijvoorbeeld: ICT) Contactperso(o)n(en) Functionaris Gegevensbescherming

5. Vaststellen meld- en herstelaanpak	- Bepaal aanpak/informeren AP - Bepaal aanpak/informeren data subject(s) - Bepaal acties voor nazorg data subject(s) - Bepaal acties voor belang van de organisatie - Bepaal acties voor verbetering beveiliging	Manager van de inhoudelijk betrokken afdeling Manager van de afdeling die verantwoordelijk is voor beveiligingsincidenten (bijvoorbeeld: ICT) Contactperso(o)n(en) Functionaris Gegevensbescherming
6. Melden bij AP *)	- Indien besloten wordt om AP te informeren dan moet dat binnen 72 uur - Melding via de website van het AP - Van tevoren kan het Meldformulier Datalekken gebruikt worden	Contactperso(o)n(en) Functionaris Gegevensbescherming Bestuur
7. Informeren data subject(s) **)	- Melding via bijvoorbeeld brief - Meedelen wat er is gebeurd, welke persoonsgegevens getroffen zijn en wat de mogelijke gevolgen van het datalek kunnen zijn. - Informeren over de maatregelen die de organisatie neemt en die de betrokkene zelf kan nemen om schade te voorkomen	Contactperso(o)n(en) Functionaris Gegevensbescherming Bestuur Marketing/communicatie
8. Uitvoeren herstelwerkzaamheden	- Herstel het datalek - Verbeteren van de beveiliging - Nazorg leveren aan data subject(s)	Manager van de afdeling die verantwoordelijk is voor beveiligingsincidenten (bijvoorbeeld: ICT) Contactperso(o)n(en)
9. Optimaliseer het proces	- Registreer, evalueer en verbeter de beveiliging, verbeter het proces, inclusief dit protocol	Contactperso(o)n(en) Functionaris Gegevensbescherming Bestuur Manager van de afdeling die verantwoordelijk is voor beveiligingsincidenten (bijvoorbeeld: ICT)

*) Melding aan de AP kan uitsluitend achterwege blijven indien het onwaarschijnlijk is dat het datalek leidt tot een verhoogd risico voor rechten en vrijheden van data subject(s). Of hiervan sprake is hangt mede af van de aard, context en omvang van de gelekte persoonsgegevens. Indien bijvoorbeeld uitsluitend de adresgegevens zijn gelekt van een kleine groep data subject(s), is het onwaarschijnlijk dat er sprake is van een verhoogd risico. Overweeg ook de context. Bijvoorbeeld: indien uitsluitend adresgegevens gelekt zijn, echter in combinatie met het herleidbare lidmaatschap van een patiënten- of cliëntenorganisatie, kan dit een gevoelig gegeven zijn. Bij de afweging van het risico voor de rechten en vrijheden van data subject(s) moet altijd de Functionaris Gegevensbescherming betrokken worden.

**) Indien aangenomen kan worden dat het datalek leidt tot een verhoogd risico voor rechten en vrijheden van data subject(s) inhoudt, dient het bovendien aan data subject(s) gemeld te worden. Het risico moet worden beoordeeld aan de hand van de aard en de hoeveelheid van de gelekte gegevens. Indien bijzondere persoonsgegevens gelekt zijn dient het lek in alle gevallen gemeld te worden bij de betrokkenen. Bij de afweging van het risico voor de rechten en vrijheden van data subject(s) moet altijd de Functionaris Gegevensbescherming betrokken worden.

ARTIKEL 5 DATA PROCESSOR

Opdrachtgever is en blijft (als gegevensverantwoordelijke) altijd eindverantwoordelijk, ook als het datalek heeft plaatsgevonden bij data processor. Dit houdt in dat ook in dit geval hetzelfde stappenplan worden afgewerkt. Data processor moet bij alle relevante stappen betrokken worden.