PRIVACY VERKLARING

ARTIKEL 1 - NOSUCH

Hier vind je de privacy verklaring van NoSuchCompany B.V., NoSuchOnsite B.V., NS+R NL B.V. en NoSuchHolding B.V., hierna te noemen NOSUCH. Hierin wordt omschreven hoe er met jouw persoonlijke gegevens om wordt gegaan die worden verzameld door NOSUCH. Zo wordt uitgelegd waar jouw gegevens opgeslagen liggen en voor welke doelen jouw gegevens opgeslagen worden. Daarnaast vind je hier ook al jouw rechten met betrekking tot jouw gegevens en hoe je gebruik kunt maken van die rechten.

Als jij je niet prettig voelt omtrent het gebruik van jouw gegevens door NOSUCH, neem dan gerust contact op!

NOSUCH
Schiehavenkade 214-222, 3024 EZ ROTTERDAM
privacy@nosuch.nl
0031 10 2441044

De privacy verklaring zal soms gewijzigd worden door bijvoorbeeld wetwijzigingen. Het is daarom raadzaam de verklaring periodiek te raadplegen.

ARTIKEL 2 - DOEL GEGEVENS

Er wordt voor een aantal doelen persoonsgegevens verzameld door NOSUCH. Hierbij wordt strikt het principe van **gegevensminimalisatie** gevolgd. Dit betekent dat alleen de minimaal noodzakelijke persoonsgegevens worden verzameld en verwerkt voor elk specifiek doel. Wij vragen en bewaren nooit meer gegevens dan nodig is om de betreffende dienst of activiteit uit te voeren.

1. Het versturen van nieuwsbrieven

NOSUCH stuurt via e-mail nieuwsbrieven. Deze nieuwsbrieven zijn enerzijds commercieel en anderzijds gericht op kennisdeling. Je naam en e-mailadres zullen worden verzameld via het daarvoor bestemde formulier op de website van NOSUCH. Daarnaast kan je mondeling of tekstueel gevraagd worden om je aan te melden voor de nieuwsbrief.

2. Het verzenden van marketing materiaal

NOSUCH verzendt marketing materiaal op aanvraag. Jouw gegevens worden verzameld als jij via de website van NOSUCH kenbaar maakt marketing materiaal te willen ontvangen. Het gaat hierbij om je naam, e-mailadres, bedrijfsnaam, functie binnen je bedrijf en de adresgegevens voor verzending.

3. Contact opnemen

Jouw gegevens zullen verzameld worden als jij contact opneemt met NOSUCH via de website. In dit formulier wordt echter alleen gevraagd om de benodigde gegevens om een voorstel of een dienst aan te kunnen bieden, zoals je naam, e-mailadres, bedrijfsnaam, telefoonnummer en omschrijving van je vraag of verzoek.

4. Analytics

De website van NOSUCH verzamelt jouw gegevens om de website te verbeteren. Dit gebeurt met Google Analytics. Deze gegevens zijn anoniem en dus niet gebonden aan jouw persoonlijke gegevens. Denk hierbij aan informatie zoals duur van je website bezoek of de pagina's die je bezoekt.

5. Sollicitaties

Via de website is er een mogelijkheid om direct te solliciteren. We vragen hierbij je naam, e-mailadres, telefoonnummer en CV. Aanvullende informatie deel je vrijwillig. Jouw gegevens worden enkel gebruikt binnen het selectieproces van de betreffende vacature.

Alle gegevens worden alleen verwerkt met jouw uitdrukkelijke toestemming, dan wel ter uitvoering van de overeenkomsten die worden aangegaan, dan wel op grond van wettelijke verplichting.

ARTIKEL 3 – GEGEVENSMINIMALISATIE EN PROPORTIONALITEIT

NOSUCH hanteert de volgende principes voor gegevensminimalisatie:

1. Minimale vereisten: Voor elke verwerkingsactiviteit worden alleen de gegevens verzameld die strikt noodzakelijk zijn voor het beoogde doel. Onnodige gegevensverzameling wordt actief vermeden.
2. Rechten en vrijheden beschermen: Bij het verzamelen en verwerken van persoonsgegevens weegt NOSUCH voortdurend af of de hoeveelheid verzamelde gegevens proportioneel is ten opzichte van de rechten en vrijheden van betrokkenen.
3. Evaluatie van verzamelde gegevens: NOSUCH voert periodiek controles uit om te waarborgen dat alleen de noodzakelijke gegevens worden verzameld en verwerkt, in overeenstemming met de doelen die in dit document zijn beschreven.
4. Verwijderen van onnodige gegevens: Persoonsgegevens die niet langer nodig zijn voor de beoogde doelen worden onmiddellijk verwijderd of geanonimiseerd, tenzij er een wettelijke verplichting is om de gegevens langer te bewaren.

ARTIKEL 4 - ONTVANGERS

De gegevens die NOSUCH ontvangt en verwerkt worden beheerd d.m.v.:

1. Campaign Monitor

De nieuwsbrieven worden verzonden met Campaign Monitor. Op het moment dat jij je aanmeldt voor de nieuwsbrief, wordt jouw e-mailadres en naam automatisch opgeslagen in de daarvoor bestemde lijst binnen Campaign Monitor.

2. Microsoft Office365

De e-mail van NOSUCH wordt gehost bij Office365. Op het moment dat jij contact opneemt via de formulieren of e-mail, worden de betreffende mails opgeslagen op de servers van Office365.

3. Savvii

De website en back-ups van de website van NOSUCH worden gehost bij Savvii. Gegevens die jij achterlaat op de website van NOSUCH zijn op de servers van Savvii opgeslagen.

4. SCORO

De project- en financiële adminstratie voert NOSUCH in SCORO. De minimaal benodigde informatie om een project te beheren en de inkoop- en verkoopfacturatie te verwerken wordt hierin opgeslagen.

5. Loket en XpertSuite

De personeelsadministratie wordt in Loket gevoerd. Hierin bevinden zich alle persoonsgegevens van onze medewerkers. De Arbodienst werkt met XpertSuite voor de verzuimbegeleiding.

6. Recruitee

Sollicitaties komen binnen in Recruitee, hierin worden de ingevoerde gegevens opgeslagen in profielen.

7. Netwerkschijf

Informatie welke niet in een systeem opgeslagen kan worden, maar wel bewaard dient te worden, wordt als een bestand opgeslagen op een centrale netwerkschijf op Microsoft Windows Server.

8. Hubspot

NOSUCH gebruikt HubSpot voor klantbeheer (CRM), marketingautomatisering en contactopvolging. Wanneer je je inschrijft voor nieuwsbrieven of interesse toont in onze diensten via de website, worden je persoonsgegevens zoals naam, e-mailadres, bedrijfsnaam en telefoonnummer opgeslagen in HubSpot. Deze gegevens worden uitsluitend gebruikt voor communicatie en marketingactiviteiten waar je expliciet toestemming voor hebt gegeven.

9. Business Monitor

NOSUCH gebruikt Business Monitor voor klant- en medewerkerstevredenheidsonderzoeken. Persoonsgegevens zoals naam, e-mailadres en feedback worden verzameld en geanalyseerd om inzichten te verkrijgen die helpen bij het verbeteren van klantbeleving en interne processen.

Business Monitor biedt veilige opslag op Nederlandse servers en werkt met realtime analyses en rapportages om resultaten inzichtelijk te maken en te optimaliseren.

ARTIKEL 5 - OPSLAGPERIODE

Jouw gegevens worden voor langere tijd bewaard door NOSUCH, maar nooit langer dan nodig is voor het uitvoeren van activiteiten, tenzij we op grond van een wettelijke regeling jouw gegevens langer moeten bewaren.

1. Het versturen van nieuwsbrieven

Jouw e-mailadres en naam worden opgeslagen in Campaign Monitor. De opslag van jouw gegevens is voor onbepaalde tijd. Jij kan je namelijk uitschrijven wanneer je maar wilt via de link onderaan de nieuwsbrieven of door een mail te sturen naar privacy@nosuch.nl. Je verzoek wordt binnen 2 werkdagen afgehandeld.

2. Het verzenden van marketing materiaal

Jouw e-mailadres, naam, bedrijfsnaam, functie en adresgegevens worden opgeslagen in Campaign Monitor. De opslag van jouw gegevens is voor onbepaalde tijd. Jij kan je namelijk uitschrijven wanneer je maar wilt door een e-mail te sturen naar privacy@nosuch.nl. Je verzoek wordt binnen 2 werkdagen afgehandeld.

3. Contact opnemen

Op het moment dat je contact opneemt met NOSUCH via mail, dan worden die gegevens die jij meestuurt, zoals bijvoorbeeld je naam, bedrijfsnaam en e-mailadres opgeslagen op de mailserver. De opslag van deze mails is voor onbepaalde tijd. Mocht je je e-mails willen laten verwijderen van deze mailserver, dan kun je dit verzoek indienen via privacy@nosuch.nl. Je verzoek wordt binnen 2 werkdagen opgevolgd.

4. Analytics

De gegevens die Google Analytics op de website verzamelt zijn anoniem, dus niet verbonden aan jouw naam, bedrijf of e-mailadres. Deze gegevens worden voor onbepaalde tijd bewaard binnen Google Analytics.

5. Recruitee

Bij een sollicitatie geef je toestemming voor een bewaartermijn van 6 maanden. Na deze 6 maanden wordt je profiel verwijderd, tenzij anders overeengekomen.

6. Hubspot

Persoonsgegevens die via HubSpot worden verzameld, zoals naam, e-mailadres en contactinformatie, worden opgeslagen zolang deze nodig zijn voor klantrelatiebeheer, marketingactiviteiten en communicatie. De gegevens worden verwijderd of geanonimiseerd zodra ze niet langer relevant zijn voor deze doeleinden, met een maximale bewaartermijn van 5 jaar, tenzij wettelijk anders vereist of de betrokkene verzoekt om verwijdering.

7. Business Monitor

Gegevens die verzameld worden via Business Monitor, zoals naam, e-mailadres en feedback, worden opgeslagen zolang deze nodig zijn voor het analyseren van klant- en medewerkerstevredenheid en voor het optimaliseren van diensten. De gegevens worden verwijderd of geanonimiseerd zodra ze niet langer relevant zijn voor deze doeleinden, met een maximale bewaartermijn van 5 jaar, tenzij wettelijk anders vereist.

ARTIKEL 6 - BEVEILIGING

Er worden van jouw persoonsgegevens geen fysieke kopieën gemaakt. Je gegevens worden alleen beheerd in de eerdergenoemde systemen en software. Uitzonderingen hierop, zoals kopieën die vereist zijn om aan wetgeving te voldoen, worden in een afgesloten ruimte bewaard en zijn enkel toegankelijk voor geautoriseerde medewerkers.

De persoonsgegevens die door NOSUCH of door eerder genoemde derden worden beheerd, zijn alleen toegankelijk via bovenstaande software en zijn beveiligd met een wachtwoord.

De apparaten die jouw gegevens openen zijn elk zelf ook vergrendeld met een wachtwoord en/of vingerafdruk. Het aantal apparaten die toegang hebben tot jouw gegevens wordt beperkt tot alleen de benodigde apparaten.

Daarnaast wordt jouw bezoek aan onze website beveiligd door een SSL certificaat. Dit betekent dat jouw verbinding met de website van NOSUCH privé is. Je herkent deze beveiliging aan het groene slotje voor de url.

In het Protocol Datalekken, opgesteld door NOSUCH en gedeeld met de medewerkers en verwerkers van onze data, staat beschreven hoe te handelen in een geval van een datalek.

ARTIKEL 7 - JOUW RECHTEN

1. Recht op inzage

Je hebt het recht om ten alle tijden jouw gegevens op te vragen die bij NOSUCH vastgelegd en bewaard worden. Dit doe je door een e-mail te sturen of telefonisch contact op te nemen met NOSUCH. Je krijgt dan een overzicht van jouw gegevens.

2. Recht op rectificatie

Kloppen je gegevens niet? Of zijn je gegevens veranderd? Je hebt het recht om dit te laten rectificeren door NOSUCH. Je gegevens omtrent de nieuwsbrief kun je aanpassen via de daarvoor bestemde url onderaan elke mail.

3. Recht op overdracht

Mocht jij de gegevens nodig hebben die bij NOSUCH opgeslagen liggen in het geval je overstapt naar een andere partij of dienst, dan heb je het recht op overdracht. Hierbij dient NOSUCH al jouw gegevens over te dragen aan de andere partij.

4. Recht op wissen van gegevens

Wil je niet langer dat jouw gegevens bij NOSUCH vastgelegd zijn? Dan heb je het recht op het laten wissen van gegevens.

5. Recht op het indienen van een klacht

Je hebt het recht om een klacht in te dienen bij Autoriteit Persoonsgegevens, als je vindt dat NOSUCH niet op de juiste manier met jouw gegevens omgaat. Dit kan via deze link.

6. Recht op stop gegevensgebruik (bezwaar)

Wil jij niet dat NOSUCH jouw gegevens gebruikt? Dan heb je het recht op het stoppen van het gebruik van jouw gegevens.

Het gebruik maken van deze rechten kan via privacy@nosuch.nl onder toezending van een kopie id-bewijs, waarbij de pasfoto, id-bewijsnummer en BSN onleesbaar zijn gemaakt. Het streven is om binnen 5 werkdagen te reageren.

ARTIKEL 8 - PLICHTEN

NOSUCH verwerkt persoonsgegevens op grond van een gerechtvaardigd belang. Denk hierbij aan het aanbieden van diensten of producten van NOSUCH via e-mail. Jouw gegevens zullen nooit verkocht worden aan derden. Zo ook andere verwerkingen die noodzakelijk zijn om onze bedrijfsactiviteiten te verrichten.

De gegevens die verplicht zijn om aan te leveren, zijn de minimale benodigde gegevens voor het aanbieden van diensten of producten. Je e-mailadres is bijvoorbeeld nodig om de nieuwsbrief te kunnen versturen. Als deze verplichte gegevens niet worden aangeleverd, kan NOSUCH de betreffende dienst niet aanbieden.

Mocht het nodig zijn de gegevens die jij hebt gedeeld met NOSUCH met anderen dan de hierboven genoemde partijen te delen (bijvoorbeeld voor het aanbieden van een dienst), dan zal daar eerst jouw toestemming voor worden gevraagd.

NOSUCH behoudt zich het recht de gegevens de gegevens te openbaren wanneer dit wettelijk is vereist dan wel wanneer NOSUCH dit gerechtvaardigd acht om te voldoen aan een juridisch verzoek/proces of om de rechten, eigendom of veiligheid van NOSUCH te beschermen. Daarbij trachten wij altijd jouw recht op privacy zoveel mogelijk te respecteren.

Heb je toch nog vragen? Neem gerust contact op via onderstaande contactgegevens.

NOSUCH
Schiehavenkade 214-222, 3024 EZ ROTTERDAM
privacy@nosuch.nl
0031 10 2441044

PROTOCOL DATALEKKEN

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 moeten elk (vermoedelijk) datalek onmiddellijk melden aan hun leidinggevende en de aangewezen Contactpersoon. Indien de Contactpersoon niet direct bereikbaar is, wordt het incident ook gemeld bij een back-up contactpersoon of de Functionaris Gegevensbescherming (FG). Leidinggevenden zijn verplicht om elke melding van een datalek te escaleren binnen één uur naar de Contactpersoon, zodat de melding binnen 72 uur kan worden beoordeeld en indien nodig kan worden gemeld 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	Bij ontdekking van een (mogelijk) datalek meldt de medewerker dit direct aan de leidinggevende én Contactpersoon. Als er geen bevestiging komt van ontvangst binnen 1 uur, neemt de medewerker contact op met de Functionaris Gegevensbescherming.	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 (leidinggevende) Manager van de afdeling die verantwoordelijk is voor beveiligingsincidenten (bijvoorbeeld: ICT) Contactperso(o)n(en)
2A. ESCALATIE BIJ ONDUIDELIJKHEID	Indien de omvang of impact van het datalek onduidelijk is, escaleert de leidinggevende binnen 1 uur naar de Functionaris Gegevensbescherming voor verdere beoordeling.	Leidinggevende Contactpersoon Functionaris Gegevensbescherming.
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.