Beleid databeveiliging en informatiebeveiliging

Stichting de Noordzee is ervan overtuigd dat de bescherming van persoonsgegevens van essentieel belang is voor haar activiteiten. Daarom wordt in dit privacy beleid heldere en transparante informatie gegeven over de wijze waarop Stichting de Noordzee persoonsgegevens verwerkt van donateurs, vrijwilligers, medewerkers en bezoekers van de website.

Persoonsgegevens van donateurs, vrijwilligers, medewerkers en bezoekers van de website worden met de grootst mogelijke zorgvuldigheid behandeld en beveiligd. Hierbij houd Stichting de Noordzee zich in alle gevallen aan de toepasselijke wet- en regelgeving, waaronder de Wet bescherming persoonsgegevens. Verantwoordelijke voor de gegevensverwerkingen is Stichting de Noordzee gevestigd Arthur van Schendelstraat 600, 3511 MJ Utrecht.

Voor welke doeleinden verwerken wij uw persoonsgegevens.

Er zijn verschillende doeleinden waarvoor Stichting de Noordzee persoonsgegevens verzamelt en verwerkt. In het kader van haar dienstverlening verzamelt en verwerkt Stichting de Noordzee persoonsgegevens:

- Voor de werving, uitvoering en voorbereiding van een donatieovereenkomst (waaronder giften) en/of anderen overeenkomst(en). In het kader van het uitvoeren van een overeenkomst kan Stichting de Noordzee, persoonsgegevens aan een derde partij, die betrokken is bij de uitvoering of precontractuele fase op verzoek van de betrokkene, verstrekken;
- Wanneer een individu contact heeft met Stichting de Noordzee. Dit contact kan telefonisch zijn (waarbij gesprekken kunnen worden gemonitord voor trainings- en kwaliteitsdoeleinden), maar hieronder wordt ook verstaan indien een individu stichting de Noordzee via e-mail benadert, gebruik maakt van de website, een inschrijving voor de nieuwsbrief ZEEmail doet of stichting de Noordzee benadert via social media;
- Bij de financiële afwikkeling van een project- of accountantscontrole;
- Van vrijwilligers van de Boskalis Beach Cleanup Tour. Vrijwilligers kunnen persoonsgegevens invullen op de website beachcleanuptour.nl. Hiermee stellen vrijwilligers de persoonsgegevens ter beschikking aan de stichting, voor dit event.

E-mail

De e-mailadressen van vrijwilligers en geïnteresseerden wordt alleen gebruikt voor het toesturen van informatie over het betreffende event of de nieuwsbrief ZEEmail. Stichting de Noordzee gebruikt deze gegevens alleen indien een individu zich heeft ingeschreven en daarvoor toestemming heeft gegeven. Die toestemming kan altijd worden intrekken door gebruik te maken van de afmeldlink in het toegezonden e-mailbericht of door een e-mail te sturen naar info@noordzee.nl onder vermelding van Wet Bescherming Persoonsgegevens.

Beleid m.b.t. veiligheid gegevens: Vereisten werknemers

Dit type beleid beschrijft het gedrag dat van werknemers wordt verwacht wanneer ze omgaan met privacy gevoelige gegevens.

Doelstelling:

Vanuit het zorgvuldigheidsprincipe en om imagoschade te voorkomen beschermt stichting de Noordzee vertrouwelijke of gevoelige gegevens tegen verlies. De beveiliging van relevante gegevens is een kritieke ondernemingsvoorwaarde, maar de flexibiliteit om gegevens te raadplegen en effectief te werken is dat ook. Er wordt niet verwacht dat de genomen maatregelen in alle gevallen doeltreffend kunnen omgaan met een scenario van moedwillige diefstal.

De primaire doelstelling is bewustzijn bij de medewerkers en scenario's van accidenteel verlies te voorkomen. Deze regels definiëren de eisen voor het voorkomen van datalekken en een richtpunt voor de regels.

Omvang:

Elke werknemer, externe medewerker of individu met toegang tot de systemen of gegevens van Stichting de Noordzee.

Beleid werknemers:

- Werknemer moet instemmen met de naleving van de arbeidsvoorwaardenregeling van Stichting de Noordzee. Deze regeling is gebaseerd op de arbeidsvoorwaarden van stichting Natuur en Milieu;
- Indien een medewerker een onbekend, niet-begeleid of niet-gemachtigd individu ziet, moet de werknemer dit direct melden bij de betreffende leidinggevende;
- Bezoekers moeten te allen tijde door een geautoriseerde werknemer worden begeleid;
- Werknemer mag het onderwerp of de inhoud van gevoelige of vertrouwelijke gegevens niet openbaar maken zonder voorafgaande toestemming;
- Om de veiligheid van gegevens te waarborgen moet de werknemer controleren dat alle relevante gedrukte gegevens niet onbewaakt op een bureau achterblijven;
- Werknemer moet alle systemen conform het wachtwoordbeleid beveiligen. Deze wachtwoordgegevens moeten uniek zijn en mogen niet voor andere externe systemen of diensten gebruikt worden;
- Werknemers waarvan het arbeidscontract beëindigd is, moeten alle records die persoonlijke gegevens bevatten, in welk formaat ook, teruggeven. Deze eis maakt deel uit van de procedure bij werving van werknemers en is opgenomen in de arbeidsvoorwaardenregeling;
- Werknemer moet onmiddellijk de directeur van stichting de Noordzee op de hoogte brengen ingeval een apparaat met relevante gegevens (bijv. mobiele telefoons, laptops enz.) verloren gaat.

Beleid m.b.t. veiligheid gegevens: Preventie van datalekken

Preventie van datalekken is bedoeld om medewerkers bewust te maken van de gegevens die worden overdragen en die beperkt of niet voor iedereen toegankelijk zijn.

Doelstelling:

Vanuit het zorgvuldigheidsprincipe en om imagoschade te voorkomen beschermt stichting de Noordzee vertrouwelijke of gevoelige gegevens tegen verlies. De beveiliging van relevante gegevens is een kritieke ondernemingsvoorwaarde, maar de flexibiliteit om gegevens te raadplegen en effectief te werken is dat ook. Er wordt niet verwacht dat de genomen maatregelen in alle gevallen doeltreffend kunnen omgaan met een scenario van moedwillige diefstal.

De primaire doelstelling is bewustzijn bij de medewerkers en scenario's van accidenteel verlies te voorkomen. Deze regels definiëren de eisen voor het voorkomen van datalekken en een richtpunt voor de regels.

Omvang:

Elk apparaat van stichting de Noordzee dat gevoelige gegevens, persoonlijk identificeerbare gegevens of bedrijfsgegevens bevat.

Het databeveiligingsbeleid van stichting de Noordzee definieert de eisen voor het omgaan met informatie en de vereiste gedragingen van werknemers externe leveranciers. Dit beleid is bedoeld om het databeveiligingsbeleid met technologische controlemiddelen te verbeteren.

Uitzonderingen: Indien er een zakelijke behoefte bestaat om dit beleid niet toe te passen (te duur, te ingewikkeld, negatieve impact op andere zakelijke noden), is de risicoanalyse van stichting de Noordzee van toepassing.

Beleid:

In aanmerking komende gegevens zijn (niet limitatief):

- Creditcardgegevens, bankrekeningnummers en andere (niet)financiële gegevens van donateurs, vrijwilligers en medewerkers;
- E-mailadressen, namen, adressen en andere combinaties van persoonlijk identificeerbare gegevens.

Externe leveranciers:

Indien afspraken met externe leveranciers worden gemaakt met betrekking tot gegevensverwerking dan wordt databeveiliging en informatiebeveiliging contractueel vastgelegd.

De gegevens en documenten van Stichting de Noordzee worden opgeslagen op Microsoft SharePoint. Binnen SharePoint heeft Stichting de Noordzee een aantal afgeschermde sites waar onder andere donateursgegevens worden opgeslagen. Deze gegevens zijn alleen toegankelijk voor de directie en een medewerker Finance.

Dagelijks wordt een back-up gemaakt van het financiële systeem. Dit gebeurt zowel op de server van de stichting als extern bij een ICT partner (Cloud). Medewerkers hebben verschillende rollen en autorisaties in het financiële systeem, niet alle gegevens zijn voor iedereen beschikbaar. Directie kan in alle modules gegevens raadplegen en heeft toegang tot de project- en urenmodule. Projectleiders hebben alleen toegang tot project- en urenmodule. De administratie heeft als enige een bewerkingsfunctie in het gehele financiële systeem. De computers en laptops waarmee gewerkt wordt hebben een logische toegangsbeveiliging met wachtwoord.

Stichting de Noordzee maakt gebruik van een nieuwsbrief: ZEEmail. Geïnteresseerden kunnen zich opgeven voor de ZEEmail via de website van de stichting. De gegevens worden opgeslagen in het online programma mailchimp. De gegevens worden beheerd door hoofd communicatie en worden alleen gebruikt voor de ZEEmail.

Gegevens van vrijwilligers van project Beach Cleanup Tour worden opgeslagen in het programma Eventbrite. Vrijwilligers vullen persoonsgegevens in op een website en stellen deze ter beschikking voor dit event. Op de projectwebsite staat een disclaimer waarvoor de gegevens gebruikt worden.

Gegevens van vrijwilligers voor Beach Cleanup Tour worden ook in een aparte beveiligde map op Microsoft Sharepoint opgeslagen. Deze map wordt beheerd door de projectleider van de Beach Cleanup Tour en hoofd communicatie. De gegevens zijn alleen op aanvraag bij de projectleider beschikbaar voor anderen medewerkers die werkzaamheden voor het project uitvoeren.