Gedragscode Databeveiliging
Veilig omgaan met informatie doen we samen

de natuur en milieufederaties

In beginsel komt het er op neer dat de NMF's geen mensen benaderen op een manier die niet mag, dat persoonsgegevens niet aan derden worden verstrekt zonder dat de 'klant' dat weet en dat het gebruik van persoonsgegevens op een veilige manier gebeurt. Wees dus 'security aware' als je met persoonsgegevens werkt, in SPITS Online en daarbuiten…

1. Wees zorgvuldig met alle informatie waarmee je in aanraking komt

a. Ga zorgvuldig om met persoonsgegevens, registreer persoonsgegevens in SPITS Online in plaats van in losse word- en excelbestanden.
b. Gooi brieven met NAWTE gegevens (naam, adres, woonplaats, telefoonnummer, e-mailadres) of andere persoonsgegevens niet in de oud papierbak, maar versnipper deze.
c. Als iemand aangeeft dat de NMF hem niet meer mag bellen, e-mailen of post toesturen, dan zijn wij verplicht om dat direct vast te leggen en daar naar te handelen. Geef dit dus door aan je secretariaat.
d. Als je een (Excel)bestand met veel persoonsgegevens moet versturen, doe het dan beveiligd met een wachtwoord en stuur het wachtwoord separaat of bel het door.
e. Neem je persoonsgegevens mee op bijvoorbeeld een USB-stick, laptop of DVD? Zorg er dan voor dat deze informatie beveiligd is.
f. Gebruik niet je privé-telefoon of laptop om persoonsgegevens van relaties van de NMF's op te slaan. Mocht dit toch nodig zijn, zorg dan dat anderen er niet bij kunnen. Neem bij voorkeur deze informatie in SPITS Online op en verwijder de informatie van je eigen telefoon of tablet.

2. Verstrek geen vertrouwelijke gegevens aan derden

a. Verstrek geen persoonsgegevens van relaties aan derden die daar geen recht op hebben. Vraag even aan de betreffende persoon of je zijn/haar gegevens mag doorgeven.
b. Het onderling uitwisselen van persoonsgegevens (bijvoorbeeld in vrijwilligersgroepen) is alleen toegestaan met toestemming van de personen die het betreft.

3. Ga zorgvuldig om met ICT-voorzieningen, voorkom ongeautoriseerde toegang

a. Vergrendel je pc (Ctrl + Alt + Delete) als je je werkplek verlaat of sluit je PC af.
b. Kies veilige wachtwoorden.
c. Bewaar wachtwoorden op een veilige plaats (zoals een wachtwoordenkluis-programma).
d. Wijzig je wachtwoorden regelmatig.
e. Laat geen papieren met persoonsgegevens onbeheerd (op je bureau) achter.
f. Leen je persoonlijke gebruikersnaam of wachtwoord niet uit, je bent altijd zelf verantwoordelijk voor het gebruik van je account (in SPITS Online) en de daarbinnen uitgevoerde acties.
g. Zet geen gevoelige persoonsgegevens (zoals een kopie paspoort of personeelsdossier) in een onbeveiligde map. Zorg ervoor dat alleen bevoegden toegang tot deze informatie (op de server) kunnen hebben.
h. Installeer geen software waarvan je de herkomst niet kent.
i. Als je je eigen ICT-middelen (bijvoorbeeld je telefoon, tablet, laptop of PC) gebruikt om toegang te krijgen tot informatie van de NMF's zorg er dan voor dat deze goed beveiligd zijn.

4. Gebruik internet, e-mail en social media met je volle verstand

a. Als je een e-mailing verstuurt naar meerdere personen (bulkmail), zet de e-mailadressen dan in de BCC en niet in de CC en richt de mail aan jezelf.
b. Als je een e-mail doorstuurt omdat je vindt dat die persoon op de hoogte moet zijn van de inhoud, zorg dan dat je de gegevens van de zender verwijdert tenzij die persoon rechtstreeks moet communiceren met de afzender.

c. Informatie van internet kan virussen of malware bevatten. Beperk je internetgebruik tot het noodzakelijke en download alleen bestanden van betrouwbare herkomst.
d. Wees bedacht op verdachte 'phishing' e-mails. Klik niet op links in deze e-mails en geef geen logingegevens af. Op internet vind je meer informatie hoe je een verdachte mail herkent.
e. Deel geen vertrouwelijke informatie via onbeveiligde media zoals e-mail, sms, of filesharing applicaties zoals Dropbox of Google Drive.
f. Plaats geen vertrouwelijke gegevens van derden op sociale netwerken zoals Facebook, Twitter of LinkedIn.
g. Let erop als je deelneemt aan een sociaal netwerk dat de NMF's niet geschaad worden door wat je plaatst.

5. Meld datalekken

a. Vanaf 1-1-2015 zijn de NMF's verplicht om "ernstige datalekken" te melden bij het AP (Autoriteit persoonsgegevens). Dus bijvoorbeeld een verloren USB-stick met persoonsgegevens moet gemeld worden, ongeacht of er misbruik van de gegevens gemaakt is. Wees eerlijk en transparant en meld het via je secretariaat aan AP mochten er gegevens "op straat komen te liggen". Geef het lek ook door aan het secretariaat van de NMF zodat we landelijk overzicht hebben en van zwakke punten kunnen leren.

6. Spreek collega's aan op onveilig gedrag

a. Bespreek zaken die je niet vertrouwt met een collega en bepaal samen welke actie je onderneemt.
b. Help collega's door ze te attenderen op situaties waarin onveilig gehandeld wordt op het gebied van het verwerken van persoonsgegevens.

7. Geef je mening over hoe gegevensbescherming veiliger kan

a. Draag verbeterpunten aan (via intranet) bij de projectgroep gegevensbeveiliging om verlies of misbruik van informatie te voorkomen.
b. Je ICT-omgeving verandert regelmatig. Denk actief mee over veiligheid van gegevens bij ingebruikname van bijvoorbeeld een nieuw systeem of een nieuwe online dienst.
c. Wees alert ('security aware').

Extra aandachtspunten (met name voor Secretariaat / Marketing / Communicatie)

a. Verzamel niet meer gegevens dan voor het doel noodzakelijk zijn.
b. Beschrijf (vooraf) in je privacy statement met welk doel je gegevens verzamelt.
c. Voor het verwerken van gegevens van jongeren onder de 16 jaar is schriftelijke toestemming van de ouder/voogd vereist.
d. Maak op je website duidelijk hoe iemand zijn persoonsgegevens kan inzien, corrigeren en verwijderen.
e. Corrigeer of verwijder de gegevens van een persoon als deze daarom vraagt.
Uitzondering is als er wettelijke verplichtingen bestaan om dat niet te doen, bijv. i.v.m. wetgeving belasting.
f. Controleer periodiek de persoonsgegevens op juistheid.
g. Vernietig de persoonsgegevens als deze niet langer noodzakelijk zijn voor de doelstellingen van de gegevensverzameling.
h. Weeg steeds het belang van de NMF af tegen de inbreuk op de privacy van de relatie.
Je mag persoonsgegevens registreren als er sprake is van een gerechtvaardigd belang. Een normale bedrijfsvoering en marketingactiviteiten vallen hier ook onder. Vraag jezelf steeds af of je het doel ook kunt bereiken zonder verwerking van persoonsgegevens of met minder persoonsgegevens. Denk vanuit degene die je benadert: hoe zou je het zelf vinden als je op deze manier benaderd werd? Bestaat er een kans dat mensen de mailing/benadering ongepast vinden? Zo ja, vraag dan vooraf eerst toestemming.
i. Je mag gegevens altijd vastleggen als je toestemming hebt gekregen. Deze toestemming moet dan wel: vooraf gegeven zijn, vrijelijk afgegeven zijn (geen vooraangevinkte vakjes), afgegeven zijn met een actieve handeling (bijv. schriftelijk of door een vinkje te plaatsen; stilzwijgen of geen actie is geen

toestemming), duidelijk omschreven zijn (concrete omschrijving van het doel en met wie de gegevens gedeeld worden).

j. Je mag persoonsgegevens delen met derden, zolang het verenigbaar is met het doel waarvoor de gegevens zijn verzameld. Vermeld in je privacyverklaring met wie je welke gegevens deelt en voor welk doel. Zorg dat er steeds sprake is van een gerechtvaardigd belang of toestemming.

k. Als iemand die niet bij de NMF werkt gegevens van de NMF verwerkt, is een bewerkersovereenkomst verplicht. Besef dat er al gauw sprake is van 'verwerken' van persoonsgegevens: het inzien van de gegevens door een externe helpdesk is al een verwerking.

Meer informatie over gegevensbescherming kun je op intranet vinden. De Projectgroep Databeveiliging werkt momenteel aan een format voor een privacy statement en een bewerkersovereenkomst. Deze zullen op intranet ter beschikking worden gesteld. Wil je daar nu al informatie over? Neem dan contact op met Sonja Rentink: info@natuurenmilieufederaties.nl.

Wij wijzen je erop dat deze gedragscode van tijd tot tijd kan worden gewijzigd. We adviseren periodiek de gedragscode na te gaan op wijzigingen. Door het ondertekenen van deze verklaring verklaar je op de hoogte te zijn van de richtlijnen over het veilig omgaan met data van de NMF's en daarnaar te handelen.

Versie 4, 19-04-2017 *Projectgroep Gegevensbescherming*

Ik heb kennis genomen van de Gedragscode Databeveiliging en zal mij daaraan houden. Deze regelingen zijn mij bij de start van mijn werkzaamheden uitgereikt dan wel vooraf toegezonden,

---

(werknemer)

_____ te _____

(datum) (plaats)