Gedragscode Privacy en informatieveiligheid

Vogelbescherming Nederland

Vogelbescherming
NEDERLAND

Gedragscode Privacy en informatieveiligheid

Vogelbescherming
NEDERLAND

Inhoudsopgave

1. Inleiding

Het is belangrijk dat er zorgvuldig met informatie van Vogelbescherming omgegaan wordt. Daarom heeft Vogelbescherming hiervoor regels opgesteld. Deze regels staan in hoofdstuk 2 van deze gedragscode.

Informatie kent vele vormen: gesprekken, papieren documenten, digitaal opgeslagen informatie, dvd's, etc. Digitale informatie kan op allerlei plekken zijn opgeslagen: pc's, laptops, telefoons, servers, websites, netwerken, usb-sticks etc.

Informatie vertegenwoordigt een waarde voor Vogelbescherming. Daarom is bescherming (beveiliging) van de informatie noodzakelijk. Voor persoonsgegevens geldt ook dat we wettelijk verplicht zijn deze veilig te beheren. Informatiebeveiliging omvat alle maatregelen die er onder andere voor zorgen dat:

- Informatie beschikbaar is;
- Informatie juist is;
- Vertrouwelijke informatie niet in verkeerde handen valt.

Informatiebeveiliging draait niet alleen om technische maatregelen. Het gedrag van iedereen die met informatie omgaat, is het belangrijkste onderdeel. Binnen Vogelbescherming gelden de volgende basisregels voor informatiebeveiliging:

1. Houd je altijd aan de wet en deze gedragscode
2. Behandel informatie met zorg
3. Draag zorg voor toegangsbeveiliging van mobiele apparatuur
4. Houd je wachtwoorden en pincodes geheim, ook voor collega's
5. Weet met wie je handelt
6. Ga zorgvuldig om met internet en e-mail
7. Meld incidenten zoals virussen, diefstal en verlies

In de gedragscode in dit document staan bovenstaande basisregels verder uitgewerkt.

Gebruikers van de (digitale) voorzieningen van Vogelbescherming zijn zelf verantwoordelijk voor hun gedrag bij het gebruik hiervan. De eigen verantwoordelijkheid geldt ook voor het omgaan met papieren informatie of informatie van Vogelbescherming op eigen digitale voorzieningen

1.1 Reikwijdte van de code

De in hoofdstuk 2 opgenomen gedragscode geldt voor iedereen die binnen Vogelbescherming activiteiten verricht of buiten Vogelbescherming informatie die betrekking heeft op activiteiten van Vogelbescherming gebruikt of verwerkt. Het gaat om zowel bedrijfsinformatie als persoons-informatie.

Medewerkers in vaste of tijdelijke dienst tekenen voor indiensttreding in de arbeidsovereenkomst voor akkoord op de gedragscode. Vrijwilligers, stagiairs en ingehuurd personeel die toegang hebben tot bedrijfsgevoelige en/of privacygevoelige gegevens moeten een geheimhoudingsverklaring tekenen, waarin ook naar deze gedragscode wordt verwezen.

1.2 Relatie met andere documenten

Informatieveiligheid geldt voor zowel persoonsgebonden als bedrijfsgevoelige informatie. Voor de persoonsgebonden informatie is een privacy statement opgesteld dat via de externe website beschikbaar gesteld wordt aan alle websitebezoekers van Vogelbescherming.

1.3 Datalekken

Wanneer data per ongeluk wordt vernietigd, gewijzigd of gewist, of wanneer er ongeoorloofd toegang tot de data wordt verkregen, dan moet dit onmiddellijk worden gemeld via compliance@vogelbescherming.nl. Het kan gaan om verlies van papieren, een USB-stick, laptop of bedrijfsgevoelige en/of privacygevoelige informatie die aan derden is verstrekt zonder dat dit de bedoeling was. Ook een hack van de website is een datalek dat onmiddellijk moet worden gemeld.

Bedrijfsgevoelige informatie

Alle bestanden van of over Vogelbescherming die als bedrijfsgevoelige informatie kan worden beschouwd.

Privacygevoelige informatie

Alle bestanden waarin persoonsgegevens voorkomen. Persoonsgegevens zijn gegevens die naar een natuurlijk persoon te zijn herleiden zoals naam, adres, woonplaats, telefoonnummer, e-mailadres, , BSN, IP-adressen, rekeningnummers, foto's, enz.

2. Gedragscode

2.1 Werkplek

- Het is niet toegestaan om beveiligingsmaatregelen van Vogelbescherming te omzeilen.
- Als je je werkplek verlaat, vergrendel je je computer met Windowstoets + L.
- Laat geen papieren of digitale gegevensdragers (USB-sticks, DVD's, etc) met privacy- en/of bedrijfsgevoelige informatie achter op je werkplek als je deze verlaat, maar leg het achter slot en grendel (clean desk).
- Beperk de opslag op USB-sticks en andere mobiele gegevensdragers tot een absoluut minimum. In ieder geval mag hier GEEN privacy- en/of bedrijfsgevoelige informatie op worden opgeslagen.
- Sla geen privacy- en/of bedrijfsgevoelige op in de netwerkmappen van Vogelbescherming, behalve waar dat uitdrukkelijk is afgeschermd voor degenen die hier voor hun werk geen toegang toe moeten hebben.
- Leen je toegangsdruppel niet uit. Dit is een strikt persoonlijke toegangssleutel.
- Laat onbevoegden niet meelopen bij het naar binnen gaan in het gebouw.
- Meld bezoekers vooraf aan en begeleid ze bij het komen en gaan.
- Laat mobiele apparatuur niet onbeheerd achter.
- Laat een collega nooit onder jouw account inloggen en werken.

2.2 Omgaan met informatie

- Informatie gebruik je alleen voor het doel waarvoor die is verstrekt.
- Informatie deel je niet met onbevoegden.
- Bedenk bij het delen van informatie telkens of er schade (financiële, imago, juridische, etc.) kan ontstaan wanneer de informatie in handen komt van anderen dan voor wie de informatie bedoeld is.
- Spreek collega's aan op het niet naleven van de regels.
- Breng geen privacy- en/of bedrijfsgevoelige informatie naar buiten.
- Verwijder documenten onmiddellijk van printers, kopieerapparaten en faxen.
- Voer vertrouwelijke documenten af in de daarvoor bestemde afgesloten afvalcontainers of de papiervernietiger.
- Weet met wie je handelt:
    - Wees je ervan bewust dat iemand kan meekijken naar documenten (ook op beeldscherm) of kan meeluisteren bij (telefoon)gesprekken.
    - Weet met wie je communiceert via telefoon, fax, internet of e-mail.
    - Gebruik je professionele oordeel wanneer je informatie krijgt: niet alles is waar.
    - Geef bij het opvragen van informatie aan waarom en door wie deze gebruikt kan worden.

2.3 Werken met je eigen apparatuur

- Je bent als gebruiker zelf verantwoordelijk voor de optimale beveiliging van de privéapparatuur (computer, laptop, smartphone, tablet, etc.) die je gebruikt voor werk gerelateerde activiteiten, zoals inloggen op de 'Huismus', andere werk gerelateerde webapplicaties en e-mail-accounts.
- Het is niet toegestaan om op je privé-apparatuur werk gerelateerde privacy- en/of bedrijfsgevoelige informatie te downloaden, op te slaan en/of te bewerken.
- Als je via je privéapparatuur (smartphone, tablet, laptop) inlogt op je e-mailaccount van Vogelbescherming, dan moet je smartphone minimaal zijn beveiligd met een wachtwoord of pincode.

2.4 Reparatie

- Het is niet toegestaan om in bruikleen verstrekte apparaten op eigen initiatief te laten repareren (zie ook je bruikleenovereenkomst). Kapotte bruikleenapparatuur moet worden ingeleverd bij Bureaumanagement.
- Als je privéapparatuur kapot is, ben je er als gebruiker zelf voor verantwoordelijk dat de reparateur via het apparaat geen toegang kan hebben tot werk gerelateerde e-mailaccounts of (web)applicaties. Let dus bijvoorbeeld op met het opslaan van wachtwoorden in webbrowsers en het toegankelijk maken van je Vogelbescherming e-mailaccount op je telefoon. Als je een kapot apparaat inclusief het wachtwoord of de inlogcode inlevert, dan kan de reparateur zich in principe toegang verschaffen tot webapplicaties waarvoor de wachtwoorden zijn opgeslagen in de webbrowser en e-mailaccounts ingesteld op de telefoon. Er is dan mogelijk sprake van een datalek, omdat de onrechtmatige verwerking van persoonsgegevens niet valt uit te sluiten. In een dergelijk geval of bij twijfel moet je dit via compliance@vogelbescherming.nl en je leidinggevende melden.

2.5 Verlies of diefstal

- Als gebruiker dien je zelf alle zorgvuldigheid in acht te nemen om diefstal of verlies van (in bruikleen gegeven) apparatuur en gegevensdragers waarop privacy- en/of bedrijfsgevoelige informatie staat, te voorkomen. Laat bijvoorbeeld apparatuur en gegevensdragers (dat is ook papieren informatie) nooit ergens liggen, zonder dat je hebt vastgesteld dat het voor onbevoegden onmogelijk is om toegang tot de informatie te krijgen.
- Verlies of diefstal van door Vogelbescherming in bruikleen gegeven apparaten of gegevensdragers altijd per direct melden bij je leidinggevende en via compliance@vogelbescherming.nl.
- Verlies of diefstal van privéapparatuur of gegevensdragers waarop onversleutelde privacy- en/of bedrijfsgevoelige werk gerelateerde informatie staat of waarmee men toegang kan krijgen tot privacy- en/of bedrijfsgevoelige werk gerelateerde informatie[1] moet je bij je leidinggevende en via de Klachten- en incidentregistratie op intranet als een beveiligingsincident aanmelden.

2.6 Accounts en wachtwoorden

- Een goed wachtwoord bestaat uit letters, cijfers en symbolen. Het wachtwoord moet minimaal 7 tekens lang zijn en mag niet eerder gebruikt zijn. Slechte wachtwoorden zijn o.a. namen, woorden uit het woordenboek, kentekens, geboortedata.
- Elke gebruiker is persoonlijk aansprakelijk voor het gebruik van accounts en wachtwoorden die door Vogelbescherming aan haar of hem zijn uitgereikt.
- Het is niet toegestaan om accountgegevens aan derden (zoals collega's, vrijwilligers, stagiaires, studenten, vrienden of familieleden) door te geven.
- Het is niet toegestaan om derden met uw persoonlijk toegewezen account toegang te verlenen tot voorzieningen van Vogelbescherming.
- Laat inloggegevens niet (op papier) rondslingeren en sla geen wachtwoorden van webapplicaties op in de webbrowser.
- Sla wachtwoorden niet onbeveiligd op een apparaat op[2].
- Betrouwbare organisaties zullen nooit om het wachtwoord vragen. Geef ze dus ook nooit af.

2.7 Internetgebruik

- Beperkt privégebruik van internet is toegestaan, mits dit niet storend is voor anderen, de dagelijkse werkzaamheden of extra belastend voor het computernetwerk.
- Het is niet toegestaan materiaal te downloaden dat teksten, afbeeldingen en/of geluid- en video-opnamen met discriminatoire of pornografische inhoud bevat, dan wel materiaal te downloaden waarvan de gebruiker redelijkerwijs kan begrijpen dat Vogelbescherming zich daar niet mee kan verenigen of de goede naam van Vogelbescherming schaadt. Bij twijfel, download dan niet.
- Het is niet toegestaan op of via de digitale omgeving van Vogelbescherming:
    - spelletjes te spelen via internet;
    - geld te verwerven, anders dan verwerving voor de doelstelling van Vogelbescherming;
    - handelingen te verrichten met een commercieel privédoel;
    - niet-organisatie gerelateerde chatrooms of fora te bezoeken;
    - zich onbevoegd toegang te verschaffen tot systemen van andere organisaties;

[1] Er is sprake van een situatie waarin toegang kan worden verkregen privacy-, en/of bedrijfsgevoelige informatie via het apparaat als bijvoorbeeld wachtwoorden van werk gerelateerde webapplicaties zijn opgeslagen in de webbrowser of toegang tot een werk gerelateerde e-mailaccount is ingesteld op de telefoon.

[2] Tip: Heb je veel wachtwoorden, maak dan gebruik van een wachtwoordmanagementapplicatie, zoals LastPass, Keepass of Dashlane.

- software, gegevens, artikelen te downloaden of te kopiëren waarvoor licenties of auteursrechten gelden.

2.8 E-mailgebruik

- Verstuur geen privacy- en/of bedrijfsgevoelige informatie onbeveiligd naar externen.[3] Is er geen alternatief, beveilig de informatie dan met een wachtwoord. Stuur het wachtwoord per sms of geef het via de telefoon door.
- Een bericht verstuurd vanaf een Vogelbescherming e-mailadres wordt door de ontvanger gezien als een e-mail van Vogelbescherming. Houdt berichten kort en zakelijk en gebruik correct Nederlands, zoals dat ook in schriftelijke communicatie gebruikelijk is.
- Gebruik één onderwerp per email en stapel geen veelvoud van onderwerpen in één e-mail. Dat bevordert de goede communicatie en voorkomt een cc-cultuur.
- Beperkt privégebruik van e-mail is toegestaan, mits dit niet storend is voor anderen of de dagelijkse werkzaamheden of extra belastend voor het computernetwerk.
- Het is niet toegestaan, dreigende (seksueel) intimiderende, (kinder-) pornografische dan wel racistische of anderszins discriminerende berichten te versturen of op te slaan.
- Het automatisch doorsturen van berichten die binnenkomen op je werk e-mailaccount naar een privé-e-mailadres is niet toegestaan. Je kunt dan immers niet controleren of er privacy- en/of bedrijfsgevoelige informatie tussen zit.
- Wees alert op berichten waarin je onder druk wordt gezet of juist wordt verleid om gegevens te verstrekken of om op een link te klikken.
- Open nooit bijlage(n) of links in een mail van onbekende afzenders. Je kunt de URL controleren door de muiscursor enkele seconden op de link laat rusten. Hierdoor kun je zien of het naar een betrouwbare site leidt. Neem bij twijfel zo snel mogelijk contact op met de helpdesk van onze ICT-provider MagnaCura (vogelbescherming@MagnaCura.nl). Beter te veel gemeld, dan niet gemeld.
- Reageer nooit op e-mails waarin wordt gevraagd om wachtwoorden en andere persoonlijke gegevens.
- Zet je afwezigheidsassistent aan als je tijdelijk geen gebruik maakt van je emailaccount.

[3] E-mail is uitgevonden in het prille begin van internet. Er is toen geen rekening gehouden met beveiliging. Een e-mail verstuurd via het internet is te vergelijken met een ansichtkaart die door iedereen die hem in handen krijgt, kan worden gelezen of zelfs veranderd. Als je een e-mail verstuurt naar een niet-Vogelbescherming e-mailadres dan is de kans groot dat de e-mail via vele mailservers gaat alvorens hij in het postvak van de geadresseerde komt. Er kan niet worden gegarandeerd dat beheerders van mailservers via welke een e-mail het postvak van de geadresseerde bereikt, de e-mails niet lezen, opslaan of veranderen.

2.9 Social Media

- Publiceer geen privacy- en/of bedrijfsgevoelige informatie.
- Verspreid geen persoonlijke informatie of foto's zonder toestemming van betreffende persoon.
- Denk goed na voordat je informatie deelt. Informatie en foto's zijn nog lange tijd vindbaar via zoekmachines.
- Respecteer je doelgroep en publiek.
- Wees nauwkeurig, check de feiten.
- Wees verantwoordelijk met wat je op social media netwerken plaatst.
- Bespreek met je leidinggevende de voorwaarden waaronder je uit naam van Vogelbescherming bevoegd bent om direct te reageren op sites en voor welke (inhoudelijke) berichten je vooraf goedkeuring nodig hebt.
- Wees duidelijk welke informatie het standpunt van Vogelbescherming bevat en welke informatie je persoonlijke visie betreft.
- Het is niet toegestaan om sollicitanten te screenen via bijvoorbeeld Social Media.

2.10 Overeenkomsten/contracten met andere partijen

- Sluit je een contract met een andere partij dan moet deze altijd door de directeur-bestuurder of het hoofd bedrijfsvoering worden getekend om rechtsgeldig te kunnen zijn.
- Is er sprake van een overeenkomst waar sprake is van uitwisselen van persoonsgegevens (personeelsinformatie, gegevens van leden of vrijwilligers) dan moet er ook een verwerkersovereenkomst worden gesloten. Is dit aan de orde, stuur dan een mail aan compliance@vogelbescherming.nl om de stukken te laten toetsen aan de AVG.

2.11 Meld incidenten en kwetsbaarheden

Jij bent als gebruiker van de informatievoorziening van Vogelbescherming medeverantwoordelijk voor de betrouwbaarheid en weerbaarheid ervan. Daarom wordt van jou veilig en integer handelen verwacht. Daarbij hoort ook dat je alert bent en zaken signaleert. Wanneer je iets afwijkends opmerkt of iets niet vertrouwt, help je mee door dit via compliance@vogelbescherming.nl en helpdesk@vogelbescherming.nl als (potentieel) beveiligingsincident te melden.
Je kunt hierbij denken aan zaken als:

- Technische incidenten, bijvoorbeeld een virus of andere malafide software.
- Een kwetsbaarheid in de digitale werkomgeving.
- Diefstal of verlies van apparatuur en informatiedragers. Zie ook §2.5.
- Inhoud van een e-mail, bijvoorbeeld aanstootgevende inhoud of mogelijke phishing[4].

[4] Phishing is een vorm van internetfraude. Het bestaat uit het oplichten van mensen door ze bijvoorbeeld met een e-mail te lokken naar een valse (bank)website, die een kopie is van de echte website, om ze daar – nietsvermoedend – te laten inloggen met hun inlognaam en wachtwoord of hun creditcardnummer. Hierdoor krijgt de fraudeur de beschikking over deze gegevens. De meeste vormen van phishing gebeuren via e-mail, maar soms wordt telefonisch contact opgenomen.