Privacyreglement Vogelaar Vredehof BV

Versie 1.0

Vastgesteld door de directie: 1 mei 2018
Inwerkingtreding: 25 mei 2018

Missie en visie

Wij bieden onze medewerkers een veilige werkplek. Daarnaast biedt Vogelaar alle betrokkenen een veilige omgeving voor de verwerking van hun persoonsgegevens. Een goede en zorgvuldige omgang met persoonsgegevens binnen Vogelaar is daarvoor een randvoorwaarde.

Met het reglement beoogt Vogelaar ervoor zorg te dragen dat in de organisatie van Vogelaar de verwerking van persoonsgegevens plaatsvindt conform de Algemene Verordening Gegevensbescherming (hierna: AVG of Verordening), de implementatiewet Verordening, sectorgedragscodes, sectorbeveiligingscodes en organisatie-specifieke (interne) regelingen.

Dit houdt onder andere in dat:

a. de persoonlijke levenssfeer van betrokkene wordt beschermd tegen onrechtmatige verwerking en/of misbruik van die gegevens, tegen verlies en tegen het verwerken van onjuiste gegevens;
b. wordt voorkomen dat persoonsgegevens worden verwerkt voor een ander doel dan het doel waarvoor ze verzameld zijn;
c. de verwerkingen niet leiden tot een hoog risico voor de betrokkenen.

Directie Vogelaar Vredehof BV

Inhoudsopgave

Artikel 1. Begripsbepalingen 4
Artikel 2. Verantwoordelijkheden 6
Artikel 3. Informatie en toegang tot de persoonsgegevens 7
Artikel 4. Categorieën van betrokkenen, doeleinden en persoonsgegevens 8
Artikel 5. Rechten betrokkenen 16
Artikel 6. Beveiliging 20
Artikel 7. De verwerker 21
Artikel 8. Inbreuk op de beveiliging 22
Artikel 9. Klachten 23
Artikel 10. Inwerkingtreding, wijziging en citeertitel 24
Bijlagenoverzicht 25
Bijlage I Protocol beveiligingsincidenten 26
Bijlage II Protocol voor het gebruik van e-mail, internet, en sociale media 29

Artikel 1. Begripsbepalingen

Voor de toepassing van dit reglement en de daarbij behorende bijlagen wordt verstaan onder:

a. *Algemene Verordening Gegevensbescherming (AVG)*: de Verordening;

b. *Autoriteit Persoonsgegevens*: toezichthoudende autoriteit, als bedoeld in artikel 51 van de AVG;

c. *bestand*: elk gestructureerd geheel van persoonsgegevens die volgens bepaalde criteria toegankelijk zijn, ongeacht of dit geheel gecentraliseerd of gedecentraliseerd is dan wel op functionele of geografische gronden is verspreid;

d. *betrokkene*: degene op wie een persoonsgegeven betrekking heeft (een sollicitant, een medewerker werkzaam/werkzaam geweest bij Vogelaar, alle overige personen werkzaam bij of ten dienste van Vogelaar, waaronder de leden van een toezichthoudend orgaan, leveranciers en dienstverleners, en tenslotte de bezoekers van één van de gebouwen van Vogelaar);

e. *derde*: degene, niet zijnde de verwerker of degene die onder gezag van de verwerkingsverantwoordelijke werkzaam zijn, die door de verwerker gemachtigd is om persoonsgegevens te verwerken;

f. *dienst van de informatiemaatschappij*: elke dienst van de informatiemaatschappij, dat wil zeggen elke dienst die gewoonlijk tegen vergoeding, langs elektronische weg, op afstand en op individueel verzoek van een afnemer van diensten wordt verricht;

g. *gegevensbeschermingseffectbeoordeling*: een beoordeling van het effect van de beoogde verwerking op de bescherming van persoonsgegevens;

h. *groep*: een economische eenheid waarin rechtspersonen organisatorisch verbonden zijn (artikel 2:24 BW);

i. *medewerkers*:
   a. de bij Vogelaar werkzame directeur en overige medewerkers;
   b. de onder a bedoelde medewerker die op welke wijze dan ook is tewerkgesteld bij of ingeleend door Vogelaar;

a. *medewerkerssnummer*: eenduidig nummer dat wordt gebruikt ten behoeve van efficiënte verwerking van persoonsgegevens;

m. *persoonsgegevens*: alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon (‘de betrokkene’);

n. *pseudonimisering*: het verwerken van persoonsgegevens op zodanige wijze dat de persoonsgegevens niet meer aan de specifieke persoon kunnen worden gekoppeld, zonder dat er aanvullende gegevens worden gebruikt, mits deze aanvullende gegevens apart worden bewaard en technische en organisatorische maatregelen worden genomen om ervoor te zorgen dat de persoonsgegevens niet aan een geïdentificeerde of identificeerbare natuurlijke persoon worden gekoppeld;

o. *Vogelaar:* Vogelaar Vredehof BV, vestiging Krabbendijke: Oude Rijksweg 13B, 4413 NA Krabbendijke, vestiging Enspijk: Polderdijk 2, 4157 JE Enspijk

p. *toestemming van betrokkene*: elke vrije, specifieke, geïnformeerde ondubbelzinnige wilsuiting door middel van een verklaring of een ondubbelzinnig actieve handeling, waarmee betrokkene hem betreffende verwerking van persoonsgegevens aanvaardt;

q. *Verordening:* Verordening EU 2016/679 van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG;

r. *verwerking van persoonsgegevens*: een bewerking of een geheel van bewerkingen met betrekking tot persoonsgegevens of een geheel van persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedés, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiding of enige andere vorm van terbeschikkingstelling, samenbrengen, met elkaar in verband brengen, afschermen, uitwissen of vernietigen van gegevens;

s. *verwerker*: degene die op basis van een overeenkomst ten behoeve van de verwerkingsverantwoordelijke persoonsgegevens verwerkt, zonder aan zijn rechtstreeks gezag te zijn onderworpen;

t. *verwerkingsverantwoordelijke*: Vogelaar.

Artikel 2. Verantwoordelijkheden

2.1. Vogelaar is verantwoordelijk voor het bepalen van het doel, de inhoud en het gebruik van de verwerking van persoonsgegevens en voor de naleving van de AVG, de bepalingen in dit reglement en het binnen de organisatie vastgestelde beleid.

2.2. Vogelaar treft maatregelen opdat persoonsgegevens, gelet op de doeleinden waarvoor zij worden verwerkt, juist en nauwkeurig zijn.

2.3. Vogelaar draagt er zorg voor dat zijn medewerkers kennis hebben van hun verantwoordelijkheden en verplichtingen bij de verwerking van persoonsgegevens.

2.4. Vogelaar informeert de beheerders en de gebruikers periodiek om te verzekeren dat ze de processen van persoonsgegevensverwerking, de daarvoor geldende regels en hun eigen rol daarin begrijpen.

2.5. Vogelaar draagt zorg voor een gegevensbeschermingseffectbeoordeling bij de verwerking van bijzondere of gevoelige persoonsgegevens die worden verwerkt met het oog op de diensten van de informatiemaatschappij of ziekteverzuim en re-integratie van medewerkers.

2.6. Vogelaar beschikt over een register van verwerkingsactiviteiten voor de gegevensverwerkingen die hij voor de verschillende categorieën van betrokkenen uitvoert.

Artikel 3. Informatie en toegang tot de persoonsgegevens

3.1. Vogelaar informeert betrokkenen voorafgaand aan de verzameling van de persoonsgegevens of, indien de gegevens van derden afkomstig zijn binnen een redelijke termijn na ontvangst, over de persoonsgegevens die worden verwerkt, met welk doel dat gebeurt, op welke grondslag, met wie de gegevens worden gedeeld (in- en extern), hoe lang en waar de gegevens worden bewaard, een algemene beschrijving van de technische en organisatorische maatregelen zoals in de AVG is voorgeschreven, informatie over eventuele doorgifte van gegevens naar landen buiten de EU, alsmede over de rechten van betrokkene op grond van de AVG.

3.2. Eenieder die betrokken is bij de uitvoering van dit reglement en daarbij de toegang krijgt tot persoonsgegevens waarvan hij het vertrouwelijke karakter kent of redelijkerwijs kan vermoeden en voor wie niet reeds uit hoofde van beroep, functie of wettelijk voorschrift ter zake van de persoonsgegevens een geheimhoudingsplicht geldt, is verplicht tot geheimhouding daarvan en tekent de geheimhoudingsverklaring. Dit geldt niet indien enig wettelijk voorschrift hem tot bekendmaking verplicht of uit zijn taak bij de uitvoering van dit reglement de noodzaak tot bekendmaking voortvloeit.

Artikel 4. Categorieën van betrokkenen, doeleinden en persoonsgegevens

4.1. Medewerkers

4.1.1. De verwerking van gegevens van medewerkers heeft ten doel:

a. het aangaan van de arbeidsovereenkomst (artikel 6 lid 1b AVG);
b. het vaststellen van het salaris en overige arbeidsvoorwaarden (artikel 6 lid 1b AVG);
c. het (laten) uitbetalen van salaris, de afdracht van belastingen en premies (artikelen 6 lid 1b en 6 lid 1c AVG);
d. de uitvoering van een voor de betrokkene geldende arbeidsvoorwaarde (artikel 6 lid 1b AVG);
e. het innen van vorderingen, waaronder begrepen het in handen van derden stellen van die vorderingen (artikel 6 lid 1b AVG);
f. het verlenen van ontslag (artikel 6 lid 1b AVG);
g. de overgang van de betrokkene naar diens (tijdelijke) tewerkstelling bij een ander onderdeel van de groep, bedoeld in artikel 2:24b van het Burgerlijk Wetboek waaraan de verwerkingsverantwoordelijke is verbonden (artikel 6 lid 1b AVG);
h. het geven van leiding en het begeleiden van betrokkene (artikel 6 lid 1b AVG);
i. het verstrekken van de bedrijfsmedische zorg voor betrokkene en het kunnen nakomen van re-integratieverplichtingen bij verzuim (artikel 6 lid 1c AVG);
j. het toegang verlenen tot het bedrijfsnetwerk (artikel 6 lid 1b AVG);
k. het regelen van en de controle van aanspraken op uitkeringen in verband met de beëindiging van een dienstverband (artikel 6 lid 1b AVG);
l. de verkiezing van de leden van een medezeggenschapsorgaan (artikel 6 lid 1c AVG);
m. het behandelen van geschillen (artikel 6 lid 1b AVG);
n. de behandeling van medewerkerszaken, anders dan genoemd onder a. t/m m. (artikel 6 lid 1b AVG);
o. het laten uitoefenen van accountantscontrole en het laten vaststellen van aanspraken op bekostiging (artikel 6 lid 1c AVG);
p. beveiliging van en toezicht op personen, zaken en gebouwen die zijn toevertrouwd aan de zorg van Vogelaar (artikel 6 lid 1f AVG);
q. het bekend maken van informatie over de organisatie op de website van de organisatie (artikel 6 lid 1f AVG).

4.1.2. Geen andere persoonsgegevens worden verwerkt dan:

a. naam, voornamen, voorletters, titulatuur, geslacht, geboortedatum, adres, postcode, woonplaats, telefoonnummer en soortgelijke voor communicatie benodigde gegevens, zoals het e-mailadres alsmede bank- en girorekeningnummer van de betrokkene;
b. BSN-nummer;
c. kopie ID-bewijs/paspoort;
d. een medewerkersnummer dat geen andere informatie bevat dan bedoeld onder a;
e. nationaliteit, geboorteplaats;
f. gegevens betreffende gevolgde en te volgen opleidingen, cursussen en stages;
g. gegevens betreffende de arbeidsvoorwaarden;
h. gegevens betreffende het berekenen, vastleggen en betalen van salarissen, vergoedingen en andere geldsommen en beloningen in natura;
i. gegevens betreffende het berekenen, vastleggen en betalen van belasting en premies;
j. gegevens betreffende de functie of de voormalige functie(s), alsmede betreffende de aard, de inhoud en de beëindiging van voorgaande dienstverbanden;
k. gegevens met het oog op de administratie van de aanwezigheid van de betrokkenen op de plaats waar de arbeid wordt verricht en hun afwezigheid in verband met verlof, arbeidsduurverkorting, bevalling of ziekte, met uitzondering van gegevens over de aard van de ziekte;
l. gegevens die in het belang van de betrokkenen worden opgenomen met het oog op hun arbeidsomstandigheden en veiligheid;
m. gegevens, waaronder begrepen gegevens betreffende gezinsleden en voormalige gezinsleden van de betrokkenen, die noodzakelijk zijn met het oog op een overeengekomen arbeidsvoorwaarden;
n. gegevens met betrekking tot de functie-uitoefening, de medewerkersbeoordeling en de loopbaanbegeleiding, voor zover die gegevens bij de betrokkenen bekend zijn;
o. inloggegevens van het bedrijfsnetwerk;
p. foto's en videobeelden met of zonder geluid van activiteiten van de organisatie;
q. camerabeelden van het bedrijfsterrein en de algemeen toegankelijke ruimten van de organisatie, te weten: Vestiging Krabbendijke: 1 camera gericht op de doks, 4 camera’s gericht op de personeelsingang, voorzijde bedrijf en inrit bedrijf aan de voorzijde. Vestiging Enspijk: geen camera’s aanwezig.
r. de gegevens met betrekking tot het tijdstip, de datum en de plaats waarop de camera-opnamen zijn gemaakt;

s. andere dan de onder a. tot en met s. bedoelde gegevens waarvan de verwerking wordt vereist ingevolge of noodzakelijk is met het oog op de toepassing van een andere niet nader genoemde wet.

4.2. Sollicitanten

4.2.1. Vogelaar heeft een sollicitatiecode (de nvp sollicitatie code: https://nvp-plaza.nl/sollicitatiecode) waarin de procedures van de organisatie inzake werving en selectie zijn opgenomen als ook de wijze van omgang met persoonsgegevens.

4.2.2. De verwerking van gegevens van sollicitanten heeft ten doel:

a. de beoordeling van de geschiktheid van betrokkene voor een functie die vacant is (artikelen 6 lid 1a en 6 lid 1b AVG);
b. de beoordeling van de geschiktheid van betrokkene voor een functie die in de nabije toekomst vacant kan komen (artikelen 6 lid 1a en 6 lid 1b AVG);
c. de afhandeling van de door de sollicitant gemaakte onkosten (artikel 6 lid 1a AVG);
d. beveiliging van en toezicht op personen, zaken en gebouwen die zijn toevertrouwd aan de zorg van Vogelaar (artikel 6 lid 1f AVG);
e. de uitvoering of toepassing van wetgeving (artikel 6 lid 1c AVG).

4.2.3. Geen andere gegevens worden verwerkt dan:

a. naam, voornamen, voorletters, titulatuur, geslacht, geboortedatum, adres, postcode, woonplaats, telefoonnummer en soortgelijke voor communicatie benodigde gegevens, zoals het e-mailadres alsmede bank- en girorekeningnummer van de betrokkene;
b. nationaliteit en geboorteplaats;
c. gegevens betreffende de godsdienst of levensovertuiging, voor zover die noodzakelijk zijn voor de beoordeling of de sollicitant voldoet aan de benoemingsvoorwaarden;
d. gegevens betreffende gevolgde en te volgen opleidingen, cursussen en stages;
e. gegevens betreffende de functie waarnaar gesolliciteerd is;
f. gegevens betreffende de aard en inhoud van de huidige dienstbetrekking, alsmede betreffende de beëindiging ervan;
g. gegevens betreffende de aard en inhoud van de vorige dienstbetrekkingen, alsmede betreffende de beëindiging ervan;
h. andere gegevens met het oog op het vervullen van de functie (bijvoorbeeld gegevens in het kader van een te voeren voorkeursbeleid voor minderheden of re-integratiebeleid);
i. camerabeelden van het bedrijfsterrein en de algemeen toegankelijke ruimten van de organisatie, te weten te weten: Vestiging Krabbendijke: 1 camera gericht op de

doks, 4 camera's gericht op de personeelsingang, voorzijde bedrijf en inrit bedrijf aan de voorzijde. Vestiging Enspijk: geen camera's aanwezig.

j. de gegevens met betrekking tot het tijdstip, de datum en de plaats waarop de camera-opnamen zijn gemaakt;

k. andere gegevens met het oog op het vervullen van de functie, die door of na toestemming van de betrokkene zijn verstrekt (assessments, psychologisch onderzoek, uitslag medische keuring);

l. gegevens verkregen uit internetsearch;

m. andere dan de onder a. tot en met m. bedoelde gegevens waarvan de verwerking wordt vereist ingevolge of noodzakelijk is met het oog op de toepassing van een andere wet.

4.3. Oud-medewerkers

4.3.1. De verwerking van gegevens van oud-medewerkers heeft ten doel:

a. het onderhouden van contacten met oud-medewerkers (artikel 6 lid 1a AVG);

b. het verzenden van informatie aan oud-medewerkers (artikel 6 lid 1a AVG);

c. het verwerken van de aanmeldingen van oud-medewerkers voor mede voor hen georganiseerde activiteiten en bijeenkomsten (artikel 6 lid 1a AVG);

d. het berekenen, vastleggen en innen van bijdragen en giften, waaronder begrepen het in handen van derden stellen van vorderingen, alsmede andere activiteiten van intern beheer (artikel 6 lid 1a AVG);

e. het doen uitoefenen van accountantscontrole (artikel 6 lid 1c AVG).

4.3.2. Geen andere persoonsgegevens worden verwerkt dan:

a. naam, voornamen, voorletters, titulatuur, geslacht, geboortedatum, adres, postcode, woonplaats, telefoonnummer en soortgelijke voor communicatie benodigde gegevens, zoals het e-mailadres alsmede bank- en girorekeningnummer van de betrokkene;

b. gegevens betreffende de functie waarin en de periode gedurende welke de oud-medewerker voor de verwerkingsverantwoordelijke werkzaam is geweest;

c. gegevens met het oog op het berekenen, vastleggen en innen van bijdragen en giften;

d. een administratiecode dat geen andere informatie bevat dan bedoeld onder a. tot en met c.;

e. gegevens met betrekking tot aanmelding activiteiten/bijeenkomsten.

4.4. Klanten

4.4.1. De verwerking van gegevens van klanten heeft ten doel:

a. het ontvangen van bestellingen of opdrachten van klanten (artikel 6 lid 1b AVG);
b. het uitvoeren van de overeenkomst of opdracht;
c. het berekenen en vastleggen van inkomsten en uitgaven en het doen van betalingen (artikel 6 lid 1b AVG);
d. het innen van vorderingen, waaronder begrepen het in handen van derden stellen van die vorderingen alsmede andere activiteiten van intern beheer (artikel 6 lid 1b AVG);
e. het onderhouden van contacten door de verwerkingsverantwoordelijke met de klanten (artikel 6 lid 1b AVG);
f. het behandelen van geschillen en het doen uitoefenen van accountantscontrole (artikel 6 lid 1c AVG);
g. de uitvoering of de toepassing van een andere wet (artikel 6 lid 1c AVG);
h. beveiliging van en toezicht op personen, zaken en gebouwen die zijn toevertrouwd aan de zorg van Vogelaar (artikel 6 lid 1f AVG).

4.4.2. Geen andere persoonsgegevens worden verwerkt dan:

a. naam, voornamen, voorletters, titulatuur, geslacht, geboortedatum, adres, postcode, woonplaats, telefoonnummer en soortgelijke voor communicatie benodigde gegevens, zoals het e-mailadres alsmede bank- en girorekeningnummer van de betrokkene;
b. gegevens met het oog op het verwerken van bestellingen of opdrachten van klanten;
c. gegevens die noodzakelijk zijn voor de uitvoering van de overeenkomst of opdracht;
d. camerabeelden van het bedrijfsterrein en de algemeen toegankelijke ruimten van de organisatie, te weten te weten: Vestiging Krabbendijke: 1 camera gericht op de doks, 4 camera's gericht op de personeelsingang, voorzijde bedrijf en inrit bedrijf aan de voorzijde. Vestiging Enspijk: geen camera's aanwezig.
e. de gegevens met betrekking tot het tijdstip, de datum en de plaats waarop de camera-opnamen zijn gemaakt;
f. andere dan de onder a. tot en met f. bedoelde gegevens waarvan de verwerking wordt vereist ingevolge of noodzakelijk is met het oog op de toepassing van een andere niet nader genoemde wet.

4.5. Bezoekers

4.5.1. De verwerking van gegevens van bezoekers van een van de gebouwen van Vogelaar heeft ten doel:

a. het interne beheer (artikel 6 lid 1f AVG);
b. beveiliging van en toezicht op personen, zaken en gebouwen die zijn toevertrouwd aan de zorg van Vogelaar (artikel 6 lid 1f AVG).

4.5.2. Geen andere persoonsgegevens worden verwerkt dan:

a. naam, voornamen, voorletters, titulatuur, geslacht, geboortedatum, adres, postcode, woonplaats, telefoonnummer en soortgelijke voor communicatie benodigde gegevens, zoals het e-mailadres alsmede de organisatie waartoe de bezoeker behoort;
b. gegevens betreffende de persoon en afdeling die de betrokkene wenst te bezoeken;
c. gegevens betreffende de datum en het tijdstip van de aankomst en het vertrek van de bezoeker;
d. camerabeelden van het bedrijfsterrein en de algemeen toegankelijke ruimten van de organisatie, te weten te weten: Vestiging Krabbendijke: 1 camera gericht op de doks, 4 camera's gericht op de personeelsingang, voorzijde bedrijf en inrit bedrijf aan de voorzijde. Vestiging Enspijk: geen camera's aanwezig.
e. gegevens met betrekking tot het tijdstip, de datum en de plaats waarop de camerabeelden zijn gemaakt;
f. andere dan de onder a. tot en met h. bedoelde gegevens waarvan de verwerking is vereist ingevolge of noodzakelijk is met het oog op de toepassing van een andere wet.

4.5.3. Website

Vogelaar informeert bezoekers van de website van Vogelaar (www.vogelaar.com) bij een bezoek aan de website over de doeleinden en gegevens die worden verwerkt bij een bezoek aan de website door middel van een privacy statement dat op de website van Vogelaar is geplaatst.

4.6. Leveranciers/dienstverleners

4.6.1. De verwerking van gegevens van leveranciers van Vogelaar heeft ten doel:

a. het doen van bestellingen of de opdrachtverlening aan dienstverleners (artikel 6 lid 1b AVG);
b. het berekenen en vastleggen van inkomsten en uitgaven en het doen van betalingen (artikel 6 lid 1b AVG);
c. het innen van vorderingen, waaronder begrepen het in handen van derden stellen van die vorderingen alsmede andere activiteiten van intern beheer (artikel 6 lid 1b AVG);
d. het onderhouden van contacten door de verwerkingsverantwoordelijke met de leveranciers (artikel 6 lid 1b AVG);
e. het behandelen van geschillen en het doen uitoefenen van accountantscontrole (artikel 6 lid 1c AVG);
f. de uitvoering of de toepassing van een andere wet (artikel 6 lid 1c AVG);
g. beveiliging van en toezicht op personen, zaken en gebouwen die zijn toevertrouwd aan de zorg van Vogelaar (artikel 6 lid 1f AVG).

4.6.2. Geen andere persoonsgegevens worden verwerkt dan:
a. naam, voornamen, voorletters, titulatuur, geslacht, geboortedatum, adres, postcode, woonplaats, telefoonnummer en soortgelijke voor communicatie benodigde gegevens, zoals het e-mailadres alsmede de organisatie waartoe de betrokkene behoort;
b. gegevens met het oog op het doen van bestellingen of het opdracht verlenen aan dienstverleners;
c. camerabeelden van het bedrijfsterrein en de algemeen toegankelijke ruimten van de organisatie, te weten te weten: Vestiging Krabbendijke: 1 camera gericht op de doks, 4 camera's gericht op de personeelsingang, voorzijde bedrijf en inrit bedrijf aan de voorzijde. Vestiging Enspijk: geen camera's aanwezig.
d. gegevens met betrekking tot het tijdstip, de datum en de plaats waarop de camerabeelden zijn gemaakt;
e. andere dan de onder a. tot en met e. bedoelde gegevens waarvan de verwerking is vereist ingevolge of noodzakelijk is met het oog op de toepassing van een andere wet.

Artikel 5. Rechten betrokkenen

5.1. Privacyverklaring

5.1.1. Vogelaar beschikt over een privacyverklaring, waarin betrokkenen in duidelijke, begrijpelijke en gemakkelijk toegankelijke vorm worden geïnformeerd over de gegevens die van hem worden verwerkt, de wijze waarop, en de redenen waarom dit gebeurt.

5.2. Recht op informatie

5.2.1. Betrokkenen van wie persoonsgegevens worden verwerkt, dan wel - indien zij de leeftijd van zestien jaar nog niet bereikt hebben - hun wettelijke vertegenwoordigers, hebben het recht van inzage in, en recht op een kopie van, de over hen, respectievelijk hun pupil, opgenomen gegevens en van de volgende informatie over:

a. de verwerkingsdoeleinden en de rechtsgrond voor de verwerking;
b. de betrokken categorieën van persoonsgegevens;
c. de ontvangers en/of categorieën van ontvangers aan wie de persoonsgegevens zijn of zullen worden verstrekt;
d. de periode gedurende welke de persoonsgegevens naar verwachting zullen worden opgeslagen of indien dat niet mogelijk is de criteria om die termijn te bepalen;
e. de herkomst van de verwerkte gegevens indien deze niet van betrokkene afkomstig zijn;
f. het bestaan van geautomatiseerde besluitvorming, alsmede het belang en de verwachte gevolgen van die verwerking voor betrokkene.

5.3. Recht op rectificatie en wissing

5.3.1. Betrokkenen hebben het recht op rectificatie van onjuiste persoonsgegevens.

5.3.2. Betrokkenen hebben recht op wissing van gegevens (‘recht op vergetelheid’) in de volgende situaties:

a. de persoonsgegevens zijn niet langer nodig;
b. de betrokkene trekt de toestemming waarop de verwerking overeenkomstig artikel 5 lid 2.a. berust in en er is geen andere rechtsgrond voor die verwerking;
c. de betrokkene maakt bezwaar tegen de verwerking en er zijn geen prevalerende dwingende vormen voor verwerking;

d. de gegevens zijn onrechtmatig verwerkt;
e. een wettelijke verplichting om de persoonsgegevens te wissen;
f. de persoonsgegevens zijn verzameld in verband met een aanbod van diensten van de informatiemaatschappij.

5.3.3. Wanneer de gegevens openbaar zijn gemaakt en Vogelaar verplicht wordt de gegevens te wissen, neemt Vogelaar, rekening houdend met de beschikbare technologie en uitvoeringskosten redelijke maatregelen waaronder technische maatregelen, om verwerkingsverantwoordelijken die de persoonsgegevens verwerken ervan op de hoogte te stellen dat de betrokkene heeft verzocht om iedere koppeling naar of kopie of reproductie van die gegevens te wissen.

5.3.4. Artikelen 6.3.1 en 6.3.2 zijn niet van toepassing als verwerking nodig is voor het uitoefenen van het recht op vrijheid van meningsuiting of voor het nakomen van een wettelijke verwerkingsverplichting, of voor het vervullen van een taak van algemeen belang, om redenen van algemeen belang op het gebied van volksgezondheid, d. met het oog op archivering in het algemeen belang wetenschappelijk of historisch onderzoek, voor zover het in 6.3.1 en 6.3.2. bedoelde recht de verwezenlijking van de deze doeleinden onmogelijk dreigt te maken of ernstig in het gedrang dreigt te brengen.

5.4. Recht op beperking van verwerking van gegevens

5.4.1. Betrokkene heeft op grond van de Verordening in nader bepaalde situaties een recht op beperking van de verwerking van zijn gegevens. Dit houdt in dat Vogelaar de persoonsgegevens, met uitzondering van de opslag, slechts verwerkt met toestemming van betrokkene of voor de instelling, uitoefening of onderbouwing van een rechtsvordering of ter bescherming van de rechten van een ander natuurlijk persoon of rechtspersoon of om gewichtige redenen van algemeen belang.

5.5. Recht op overdraagbaarheid van gegevens

5.5.1. Betrokkene heeft recht de hem betreffende persoonsgegevens die hij zelf aan Vogelaar heeft verstrekt in een gestructureerde, gangbare en machineleesbare vorm te verkrijgen en hij heeft het recht die gegevens aan een andere verwerkingsverantwoordelijke over te dragen in de gevallen dat persoonsgegevens door hem op basis van verleende toestemming (ar-

tikel 6 lid 1 a AVG) zijn verstrekt of op basis van een overeenkomst (artikel 6 lid 1 b AVG) en de verwerking via geautomatiseerde procedés wordt verricht.

5.5.2. Bij de uitoefening van zijn recht op gegevensoverdraagbaarheid uit hoofde van het vorige lid heeft de betrokkene het recht dat gegevens indien dit technisch mogelijk is rechtstreeks van de ene naar de andere verwerkingsverantwoordelijke worden doorgezonden.

5.5.3. Het recht geldt niet voor verwerkingen die noodzakelijk zijn voor de vervulling van een taak van algemeen belang of van een taak in het kader van de uitoefening van het openbaar gezag dat aan de verwerkingsverantwoordelijke is verleend.

5.6. Indiening van een verzoek

Een verzoek als bedoeld in dit artikel wordt gericht aan Vogelaar ter attentie van Hermen van der Meijden: 0113-397114 / hermen@vogelaar.com of Nanda de Leeuw: 0113-397124 / nanda@vogelaar.com.

5.6.1. Aan een verzoek zijn geen kosten verbonden. Wanneer verzoeken van een betrokkene kennelijk ongegrond, of buitensporig zijn, met name vanwege hun repetitieve karakter kan Vogelaar echter:

- een redelijke vergoeding aanrekenen in het licht van de administratieve kosten waarmee het verzoek gepaard gaat; ofwel
- weigeren gevolg te geven aan het verzoek.

5.6.2. Vogelaar verstrekt de betrokkene binnen een maand na ontvangst van het verzoek informatie over het gevolg dat aan het verzoek is gegeven.

5.6.3. Indien de betrokkene een verzoek doet omdat bepaalde opgenomen gegevens onjuist c.q. onvolledig zouden zijn, hij een belang heeft bij beëindiging van de verwerking dat zwaarder weegt dan dat van de organisatie, dan wel de verwerking gezien de doelstelling van het reglement niet (langer) noodzakelijk is, dan wel strijdig is met dit reglement, neemt de verwerkingsverantwoordelijke binnen een maand nadat betrokkene dit verzoek heeft ingediend, hierover een schriftelijke beslissing.

5.6.4. Afhankelijk van de complexiteit van de verzoeken en van het aantal verzoeken kan die termijn indien nodig met nog eens twee maanden worden verlengd. Vogelaar stelt de betrok-

kene binnen een maand in kennis van een dergelijke verlenging. Wanneer betrokkene zijn verzoek elektronisch indient, wordt de informatie indien mogelijk elektronisch verstrekt, tenzij de betrokkene anderszins verzoekt.

5.6.5. Indien Vogelaar twijfelt aan de identiteit van de verzoeker, vraagt hij zo spoedig mogelijk aan de verzoeker schriftelijk nadere gegevens inzake zijn identiteit te verstrekken of een geldig identiteitsbewijs te overleggen. Door dit verzoek wordt de termijn voor behandeling van het verzoek opgeschort tot het tijdstip dat het gevraagde bewijs is geleverd.

5.6.6. Indien Vogelaar geen gevolg wenst te geven aan een verzoek als bedoeld in dit artikel doet hij hiervan – gemotiveerd - schriftelijk mededeling aan de betrokkene, binnen een maand na ontvangst van het verzoek.

5.7. Beperkingen

5.7.1. De reikwijdte van verplichtingen van Vogelaar enerzijds en de rechten van betrokkene anderzijds kunnen zijn beperkt op grond van wet- en regelgeving die op Vogelaar en/of zijn verwerkers van toepassing zijn.

5.8. Recht op het indienen van een klacht

5.8.1. De betrokkene die zich niet kan verenigen met de afwijzing van zijn verzoek als bedoeld in dit artikel kan zich wenden tot de klachtencommissie zoals bedoeld in de klachtenregeling van Vogelaar of de Autoriteit Persoonsgegevens benaderen met een verzoek tot bemiddeling.

Artikel 6. Beveiliging

6.1. Vogelaar zorgt voor passende beveiligingsmaatregelen en een passend beveiligingsniveau, rekening houdend met de stand der techniek en de kosten van de tenuitvoerlegging gelet op de risico's die de verwerking en de aard van de te beschermen gegevens met zich meebrengen. De maatregelen zijn er mede op gericht onnodige verzameling en verdere verwerking van persoonsgegevens te voorkomen.

Artikel 7. De verwerker

7.1. De verwerkers zijn degenen die op basis van een overeenkomst voor of namens Vogelaar gegevens verwerken.

7.2. De verwerker verwerkt de gegevens op de wijze zoals overeengekomen in een verwerkersovereenkomst.

7.3. De verwerker is verantwoordelijk voor het juiste gebruik van de nodige voorzieningen om de bescherming van de persoonlijke levenssfeer van de personen van wie gegevens in de persoonsregistratie zijn opgenomen, in voldoende mate te waarborgen, zoals aangegeven en beschreven in de verwerkersovereenkomst.

7.4. Vogelaar ziet erop toe dat de in het vorige lid bedoelde voorzieningen worden getroffen en in acht worden genomen.

Artikel 8. Inbreuk op de beveiliging

8.1. Indien zich binnen de organisatie van Vogelaar of bij een door Vogelaar ingeschakelde verwerker een inbreuk op de beveiliging voordoet, waarbij een aanzienlijke kans bestaat op verlies of onrechtmatige verwerking van persoonsgegevens die door Vogelaar worden verwerkt, dan wel dit verlies of onrechtmatige verwerking zich daadwerkelijk voordoet, zal Vogelaar daarvan melding doen bij de Autoriteit Persoonsgegevens, tenzij kan worden aangetoond dat het onwaarschijnlijk is dat deze inbreuk risico's voor de rechten en vrijheden van natuurlijke personen met zich brengt.

8.2. Vogelaar zal iedere inbreuk op de beveiliging als bedoeld in artikel 9.1. documenteren, ongeacht of deze wordt gemeld bij de Autoriteit Persoonsgegevens.

8.3. Indien de inbreuk een hoog risico voor de rechten en vrijheden van betrokkene inhoudt, stelt Vogelaar ook de betrokkene onverwijld in kennis van de inbreuk. Deze mededeling kan achterwege blijven indien:

- de persoonsgegevens versleuteld zijn en niet toegankelijk voor derden;
- er inmiddels maatregelen getroffen zijn die het hoge risico hebben weggenomen;
- de mededeling een onevenredige inspanning vergt. Een openbare mededeling kan dan volstaan.

8.4. Bij het vaststellen of sprake is van een inbreuk op de beveiliging en of melding daarvan moet worden gedaan bij de Autoriteit Persoonsgegevens hanteert Vogelaar de procedures die zijn opgenomen in het handboek en protocol Datalekken. Zie bijlage I.

Artikel 9. Klachten

9.1. Indien de betrokkene van mening is dat de bepalingen van de AVG-Verordening en/of overige wet- en regelgeving en/of gedragscodes zoals uitgewerkt in dit reglement niet door de instelling worden nageleefd dient hij/zij zich te wenden tot Hermen van der Meijden: 0113-397114 / hermen@vogelaar.com of Nanda de Leeuw: 0113-397124 / nanda@vogelaar.com.

9.2. Indien de ingediende klacht voor de betrokkene niet leidt tot een voor hem/haar acceptabel resultaat, kan hij/zij zich wenden tot de Autoriteit Persoonsgegevens dan wel tot de rechter.

Artikel 10. Inwerkingtreding, wijziging en citeertitel

10.1. Dit reglement kan aangehaald worden als '*Privacyreglement Vogelaar*' en treedt in werking op de datum vermeld op het titelblad.

10.2. Het reglement is vastgesteld door Vogelaar Vredehof BV en vervangt eventuele vorige versies.

10.3. Het reglement zal periodiek worden geëvalueerd en kan indien dit wordt gewenst of nodig is om de AVG correct na te leven, worden gewijzigd.

Bijlagenoverzicht

Bijlage I	Handboek datalekken
Bijlage II	Protocol gebruik van e-mail, internet en sociale media

Bijlage I Protocol beveiligingsincidenten

Artikel 1. Doel van dit protocol

Het doel van dit protocol is tweeledig. Enerzijds dient het een medewerker bewust te maken wat een inbreuk op de beveiliging is of kan zijn en anderzijds dient het de medewerker te informeren op welke wijze hij een mogelijk beveiligingsincident (dat mogelijk tevens een datalek blijkt te zijn) dient te signaleren.

Artikel 2. Begripsbepalingen

1.	Medewerker(s):	medewerkers als bedoeld in hoofdstuk 3 van het Handboek Datalekken;
2.	beveiligingsincident:	is een inbreuk op de beveiliging die mogelijk leidt tot het verlies of onrechtmatige verwerking van persoonsgegevens;
3.	datalek:	is een inbreuk op de beveiliging die wel leidt tot het verlies of onrechtmatige verwerking van persoonsgegevens;
4.	persoonsgegevens:	de gegevens als bedoeld in artikel 1 van het Privacyreglement;

Artikel 3. Meldplicht datalekken

Sinds 1 januari 2016 dient een verwerkingsverantwoordelijke een zogenaamd datalek onverwijld te melden aan de Autoriteit Persoonsgegevens (AP) en mogelijk ook aan de betrokkene(n). Van een datalek dat moet worden gemeld is sprake indien er persoonsgegevens verloren gaan of onrechtmatig worden verwerkt en het waarschijnlijk is dat de inbreuk een risico inhoudt voor de rechten en vrijheden van betrokkene(n).

In het kader van deze wettelijke plicht heeft de organisatie een Handboek Datalekken opgesteld en geïmplementeerd. Onderdeel daarvan is ook dit protocol. Als het organisatiebestuur namelijk niet op de hoogte is van een mogelijk beveiligingsincident zal het Handboek Datalekken niet in werking (kunnen) treden. Het organisatiebestuur is dan ook afhankelijk van de input die zij in dit verband krijgt van onder andere de medewerkers.

Artikel 4. Meldingsplicht medewerkers

Een medewerker is verplicht een (mogelijk) beveiligingsincident dat hij/zij ontdekt direct per e-mail of telefonisch te melden aan de HR manager ongeacht het tijdstip van de dag. Deze melding zal zo concreet mogelijk zijn. De medewerker neemt daarbij de inhoud van dit protocol in acht.

In dit verband geldt dat een medewerker bij twijfel of er sprake is van een mogelijk beveiligingsincident toch meldt aan de HR Manager.

Artikel 5. Persoonsgegevens

Wat zijn persoonsgegevens? Dit zijn niet alleen gegevens zoals naam, adres, woonplaats of BSN-nummer. Deze gegevens worden aangeduid als direct identificerende gegevens. Daarnaast zijn er ook indirect identificerende gegevens. Dit zijn gegevens die iets zeggen over een natuurlijk persoon omdat zij gekoppeld kunnen worden aan een direct persoonsgegeven. Indien kan worden achterhaald om welke natuurlijke persoon het gaat, is er sprake van een persoonsgegeven. Het kan dus onder andere gaan om:

- naam;
- adres;
- telefoonnummer;
- e-mailadres;
- salarisgegevens;
- gegevens met betrekking tot ziekte;
- beoordelingsgesprekken;
- gegevens met betrekking tot gezondheid;
- dyslexie;
- betalingsachterstanden;
- gegevens over gezinssituatie;
- geloof;
- ras;
- etc.

Artikel 6. Soorten beveiligingsincidenten

Er zijn verschillende soorten beveiligingsincidenten. Sommige beveiligingsincidenten zijn het gevolg van menselijke fouten, onoplettendheid of technisch falen. Deze beveiligingsincidenten worden niet bewust gecreëerd. Veel beveiligingsincidenten worden echter bewust gecreëerd.

Niet bewuste incidenten
Bij niet bewuste beveiligingsincidenten gaat het om incidenten die niet met opzet worden gecreeerd. Te denken valt aan:

- het laten liggen door van een laptop, tablet, smartphone of papieren dossier in de trein;
- het verliezen van een USB-stick, mobiele telefoon of bijvoorbeeld laptop;
- door haperende beveiliging (technische storing) zijn mogelijk persoonsgegevens ingezien door onbevoegden;
- de ruimte op organisatie met daarin de fysieke personeelsdossiers heeft per ongeluk niet op slot gezeten voor een bepaalde periode;
- een personeelslid heeft per ongeluk onbeheerd zijn laptop laten staan met daarop een memo-sticker met zijn inlognaam en wachtwoord;
- het verzenden door een medewerker van e-mail met vertrouwelijke gegevens aan de verkeerde ontvanger;
- het verzenden van een e-mail aan meerdere ontvangers die elkaars emailadressen niet kennen (zonder gebruik te maken van de bcc-optie);
- het crashen van een harde schijf met daarop persoonsgegevens;
- brand in een serverruimte of archiefruimte van de organisatie;
- één van de hier voor genoemde situaties zich voordoet bij een verwerker van de organisatie (bijvoorbeeld: de salarisadministratie) voor zover het persoonsgegevens betreft van personeel van de organisatie.

<u>Bewuste incidenten</u>
Bij bewuste beveiligingsincidenten gaat het om incidenten die met opzet worden gecreëerd. Te denken valt aan:

- fysieke diefstal van een laptop, tablet, smartphone of (onderdelen van een) papieren dossier;
- het kopiëren, meenemen of bijvoorbeeld vernietigen van persoonsgegevens door personeel bijvoorbeeld uit onvrede over ontslag, als vriendendienst of als gevolg van chantage;
- phishing: het uitbuiten van menselijke kwetsbaarheden door hen onder valse voorwendselen persoonsgegevens te ontfutselen via mail of internet;
- hack: het uitbuiten van kwetsbaarheden in informatiesystemen en webservers;
- één van de hier voor genoemde situaties zich voordoet bij een verwerker van de organisatie voor zover het persoonsgegevens betreft van personeel van de organisatie.

  Indien zich een dergelijk onbewust of bewust gecreëerd incident – of soortgelijkend incident – voordoet, is er sprake van een beveiligingsincident en dient de medewerker dit te melden aan Hermen van der Meijden: 0113-397114 / hermen@vogelaar.com of Nanda de Leeuw: 0113-397124 / nanda@vogelaar.com.

Bijlage II Protocol voor het gebruik van e-mail, internet, en sociale media

Artikel 1 Werkingssfeer van deze regeling, begrippen

1.1 Deze regeling geeft de wijze aan waarop binnen Vogelaar wordt omgegaan met informatie- en communicatietechnologie (hierna: ICT). Deze regeling omvat (gedrags)regels ten aanzien het gebruik van de ICT en geeft regels voor welke doeleinden en op welke wijze controle plaats vindt op dit gebruik.

1.2 Deze regeling geldt voor eenieder die ten behoeve van de organisatie werkzaamheden verricht (medewerkers, maar bijvoorbeeld ook: stagiaires en vrijwilligers). Gezamenlijk worden zij in dit reglement ook aangeduid als 'gebruiker(s)'.

1.3 Elke nieuwe gebruiker wordt gewezen op de toepasselijkheid van deze regeling. Daarbij wordt aangegeven waar de volledige tekst van deze regeling geraadpleegd/ingezien kan worden. Alle medewerkers ontvangen eens per jaar een herinnering aan de geldende regels.

1.4 Voor zover de gebruikers thuis of elders gebruik maken van de ICT (bijvoorbeeld het e-mailadres van de organisatie of de organisatiewebsite) zijn de bepalingen van deze regeling eveneens van toepassing.

Artikel 2 Toegang tot en gebruik van de ICT

2.1 Vogelaar geeft de gebruiker het recht op toegang tot de ICT (en de daarmee verbonden systemen en faciliteiten), maar behoudt zich het recht voor de toegang weer in te trekken.

2.2 Gebruikersidentificatie (gebruikersnaam) en authenticatie (wachtwoord) worden door de ICT-afdeling verstrekt en zijn persoonsgebonden en mogen niet aan anderen worden doorgegeven.

2.3 Het is gebruiker niet toegestaan om persoonsgegevens die gebruiker ter beschikking staan voor de uitoefening van zijn functie lokaal op te slaan (dus niet op het computernetwerk) noch op privé-apparatuur, tenzij daarvoor voorafgaande toestemming is verleend door diens leidinggevende en adequate waarborgen zijn getroffen voor de beveiliging van de persoonsgegevens.

Artikel 3 Gebruik van de ICT-apparatuur

3.1 De gebruiker dient zorgvuldig om te gaan met de ICT-apparatuur, zodat deze niet beschadigd raakt. De apparatuur dient in goede orde te worden achtergelaten. Eventuele schade of ontbreken van onderdelen dient direct gemeld te worden aan de ICT-afdeling.

3.2 Alleen de ICT-afdeling is bevoegd om apparatuur te ontkoppelen, verplaatsen of aan te sluiten aan het organisatienetwerk of aan apparatuur die aan het organisatienetwerk verbonden is.

3.3 De ICT-afdeling verleent alleen ondersteuning op apparatuur die door de ICT-afdeling is aangeschaft, aangesloten en geïnstalleerd.

3.4 Het gebruik van eigen opslagmedia (bijvoorbeeld: een USB-stick) van de gebruikers is toegestaan, mits onder de volgende voorwaarden:

a) voor het correct laten functioneren van het opslagmedium kan geen beroep worden gedaan op de ICT-afdeling;

b) de bestanden en programmatuur die op het opslagmedium staan moeten voldoen aan de voorwaarden zoals vastgelegd in dit reglement.

3.5 Het gebruik van eigen computerapparatuur (bijvoorbeeld laptops of tablets) is toegestaan onder de volgende voorwaarden:

a) Voorafgaand aan het gebruik is toestemming verleend door de leidinggevende en is contact opgenomen met de ICT-afdeling. Deze is bevoegd om, met opgaaf van redenen, de apparatuur niet toe te staan;

b) de gebruiker geeft de ICT-afdeling de gelegenheid om voorafgaand aan het gebruik maatregelen te treffen om de beheersbaarheid en de veiligheid te waarborgen;

c) het gebruik van de betreffende apparatuur moet voldoen aan de voorwaarden zoals vastgelegd in dit reglement.

Artikel 4 Toegang tot en gebruik van internet en e-mail

4.1 Vogelaar behoudt zich het recht voor om de toegang tot bepaalde sites door middel van een filtersysteem te beperken.

4.2 Het versturen van e-mailberichten moet voldoen aan de volgende algemene voorwaarden:

a) de afzender wordt correct weergegeven;

b) duidelijke onderwerp aanduiding;

c) terughoudend omgaan met vertrouwelijke gegevens en gevoelige informatie.

4.3 Voor het verzenden en ontvangen van e-mail binnen de organisatie wordt alleen gebruik gemaakt van de e-mailprogrammatuur die de organisatie hiervoor beschikbaar stelt. Het gebruik van andere mailprogrammatuur is niet toegestaan.

Artikel 5 (On)verantwoord gebruik van de ICT

Verantwoord gebruik

5.1 Als uitgangspunt geldt dat het gebruik van de ICT van de organisatie ten dienste moet staan aan de werkzaamheden van de gebruiker of de organisatie. Indien en voor zover sprake is van het verwerken van persoonsgegevens gebeurt dit met inachtneming van het Privacyreglement.

5.2 Gebruikers mogen de ICT beperkt, incidenteel en kortstondig gebruiken voor persoonlijke doeleinden, mits dit niet storend is voor de dagelijkse werkzaamheden of het systeem en mits hierbij wordt voldaan aan de verdere regels van deze regeling.

Onverantwoord gebruik

5.3 Het is niet toegestaan om de ICT zodanig te gebruiken dat het systeem- en/of de beveiliging opzettelijk worden aangetast.

5.4 Het is niet toegestaan zich toegang te verschaffen tot gegevens van andere gebruikers, tenzij met uitdrukkelijke toestemming van de betreffende gebruiker.

5.5 Het is niet toegestaan pogingen te ondernemen om het filtersysteem te omzeilen.

5.6 Het is in het bijzonder niet toegestaan om:

a) sites te bezoeken die pornografisch, racistisch, discriminerend, (seksueel) intimiderend, beledigend of aanstootgevend materiaal bevatten;

b) pornografisch, racistisch, discriminerend, (seksueel intimiderend, beledigend of aanstootgevend materiaal te bekijken of te downloaden of te verspreiden;

c) zich tot niet-openbare bronnen op het netwerk, internet of andere computernetwerken toegang te verschaffen en bewust informatie waartoe men via de ICT oneigenlijk toegang heeft verkregen zonder toestemming te veranderen of te vernietigen;

d) bestanden te downloaden en/of op het computernetwerk of lokaal op een PC van de organisatie te plaatsen die geen verband houden met studie en/of werk;

e) software en applicaties te downloaden en/of te installeren zonder voorafgaande toestemming van de ICT-afdeling;

f) spelletjes te spelen;

g) anoniem of onder een fictieve naam via de ICT te communiceren;

h) op dreigende, beledigende, seksueel getinte, racistische dan wel discriminerende manier via de ICT te communiceren;

i) inkomende privé-berichten te genereren door het deelnemen aan niet-zakelijke nieuwsgroepen, abonnementen op e-zines, elektronisch winkelen, down- en uploaden van bestanden, nieuwsbrieven en dergelijke;

j) kettingmailberichten en andere berichten die verstopping veroorzaken of het werk van anderen verstoren te verzenden of door te sturen;
k) iemand lastig te vallen via de ICT;
l) het introduceren en verspreiden van computervirussen en andere software die de integriteit van de gegevens of de computerbeveiliging van de ICT kunnen beschadigen;
m) gebruik te maken van chatvoorzieningen.

5.7 Het is niet toegestaan om foto's, video's of ander materiaal van bij de organisatie werkzame personen of andere bij de organisatie betrokkenen via de ICT (daaronder ook begrepen: social media) te publiceren, tenzij dit gericht is op een aan de organisatie gerelateerde doelstelling en de afgebeelde personen hebben aangegeven in te stemmen met dergelijke publicaties.

5.8 Het is ook anderszins niet toegestaan om door middel van de ICT in strijd met de wet of onethisch te handelen.

5.9 De organisatie kan de ICT-afdeling opdracht geven geconstateerde ongeoorloofde data van het computernetwerk te verwijderen.

5.10 Het is voor testdoeleinden toegestaan software lokaal te installeren die nodig is voor de werkzaamheden ten behoeve van de organisatie.

5.11 Een vermoeden van misbruik van ICT en inbreuken op de beveiliging, van binnenuit of van buiten de organisatie dienen onmiddellijk aan de ICT-afdeling gemeld te worden, hieronder vallen tevens inbreuken op de beveiliging die bij toeval worden ontdekt.

5.12 Als de gebruiker eraan twijfelt of een bepaald gebruik van ICT wel verantwoord is, dan overlegt hij daarover met de ICT-afdeling.

Artikel 6 Algemene uitgangspunten van controle op gebruik

6.1 Vogelaar heeft er recht op en belang bij dat zij het gebruik van de ICT door gebruikers kan controleren. De controle op gebruik van de ICT zal overeenkomstig deze regeling uitgevoerd worden. Als zich situaties voordoen waarin deze regeling niet voorziet, dan zal conform de Algemene Verordening Gegevensbescherming (AVG) gehandeld worden.

6.2 Als Vogelaar merkt of erop geattendeerd wordt dat het ICT-gedrag van een gebruiker niet binnen de kaders van dit reglement verloopt, wordt de gebruiker hierop door de organisatie gewezen en wordt een controle van zijn ICT-gebruik door bevoegde personen van de ICT-afdeling als mogelijkheid genoemd.

6.3 Gestreefd wordt naar een goede balans tussen enerzijds controle op het gebruik van de ICT en anderzijds de bescherming van de privacy van gebruikers.

6.4 Controle op het gebruik van de ICT zal waar mogelijk zoveel mogelijk geautomatiseerd plaatsvinden, waarbij in geval van verdachte berichten, het bericht geautomatiseerd wordt

teruggezonden aan de verzender. Voor zover geautomatiseerde controle niet mogelijk, dan wel ontoereikend is, zal de controle op het gebruik van de ICT in beginsel steekproefsgewijs plaatsvinden.

6.5 In geval dat ten aanzien van een gebruiker, vanwege een concreet vermoeden van oneigenlijk gebruik, een gerichte controle is uitgevoerd, stelt de organisatie deze gebruiker daarvan zo spoedig mogelijk nadat de controle heeft plaatsgevonden van op de hoogte.

6.6 Persoonsgegevens met betrekking tot het gebruik van ICT worden niet langer bewaard dan noodzakelijk, met een bewaartermijn van [zes maanden].

6.7 Privémail/-gebruik (voorzien van het label 'persoonlijk') wordt zoveel mogelijk ontzien van controle.

6.8 Elektronische informatie- en communicatieberichten van vertrouwenspersonen en andere personeelsleden met een vertrouwensfunctie, gecommuniceerd in het kader van hun functie, zijn uitgesloten van inhoudelijke controle.

6.9 De organisatie treft voorzieningen voor de positie en de integriteit van de ICT-afdeling. De medewerkers van de ICT-afdeling hebben een geheimhoudingsplicht die inhoudt dat ten aanzien van de verzamelde en voor hen inzichtelijke informatie strikte geheimhouding betracht dient te worden.

Artikel 7 Doeleinden van controle

7.1 De controle op persoonsgegevens bij gebruik van de ICT vindt slechts plaats met als doel:

a) het tegengaan van onverantwoord en ontoelaatbaar gebruik;
b) de naleving van het Privacyreglement;
c) het bewaken van de voortgang van werkzaamheden;
d) het vastleggen van bewijs en/of archief;
e) de systeem- en netwerkbeveiliging;
f) de kosten- en capaciteitsbeheersing.

7.2 Onder 'onverantwoord en ontoelaatbaar gebruik' als bedoeld in artikel 7.1 wordt begrepen: het onverantwoord gebruik als opgenomen in artikelen 5.3 tot en met 5.11.

7.3 Onder 'bewaking van de voortgang van de werkzaamheden' als bedoeld in artikel 7.1 wordt begrepen: controle op de inhoud van zakelijke e-mails van gebruikers voor wie het communiceren per e-mail rechtstreeks met de te verrichten taken verband houdt. Middels deze controle kan de voortgang van de werkzaamheden worden gegarandeerd bij ziekte of afwezigheid van de medewerker.

7.4 Onder 'vastleggen van bewijs en/of archief' als bedoeld in artikel 7.1 wordt begrepen: het maken van kopieën van e-mails vanuit de behoefte aan bewijs voor zakelijke transacties en dossiervorming (al dan niet met het oog op het voeren van juridische procedures).

7.5 Onder ‘systeem- en netwerkbeveiliging’ als bedoeld in artikel 7.1 wordt begrepen: controle op het e-mail- en internetgebruik ter voorkoming van systeemaanvallen door onder andere virussen, trojans of andere schadelijke programma’s.

7.6 Onder ‘kosten- en capaciteitsbeheersing’ als bedoeld in artikel 7.1 wordt begrepen: controle op het e-mail- en internetgebruik ter inventarisering en/of beheersing van de kosten die gemoeid zijn met het gebruik van de ICT.

Artikel 8 Specifieke uitgangspunten van controle op gebruik

8.1 In het kader van de controle op de gebruikers voor het doel als bedoeld in artikel 7.1.a geldt dat:

a) controle op de naleving van de regels in beginsel geautomatiseerd en steekproefsgewijs plaatsvindt;

b) indien er een concreet vermoeden is dat een gebruiker de regels, waarvan de naleving wordt gecontroleerd, overtreedt, zo nodig een in tijd en omvang zo beperkt mogelijke gerichte controle op persoonsniveau plaatsvindt;

c) daarbij worden in eerste instantie de berichten en/of het surfgedrag gescreend op (onder andere) verdachte afzender(s), bestemming, website, verdacht onderwerp, verdachte zoekopdracht, verboden woord in de inhoud of verboden extensies van de bijlage(n);

d) vervolgens worden de berichten, waarvan aannemelijk is dat het regulier verkeer betreft of waartegen ook overigens geen bedenkingen bestaan, ongeopend doorgezonden (bij originelen) of vernietigd (kopieën);

e) de overgebleven berichten kunnen worden geopend voor nader inhoudelijk onderzoek.

8.2 In het kader van de controle voor het doel als bedoeld in artikel 7.1.b geldt dat slechts berichten worden verwerkt die rechtstreeks verband houden met uitvoering van de te verrichten taken door de gebruiker.

8.3 In het kader van de controle voor het doel als bedoeld in artikel 7.1.b geldt dat slechts de e-mailverkeersgegevens en inhoud van de berichten wordt verwerkt.

8.4 In het kader van de controle voor het doel als bedoeld in artikel 7.1.c geldt dat slechts zakelijke berichten worden verwerkt voor zover deze kunnen dienen als bewijs van zakelijke transacties en dossiervorming.

8.5 In het kader van de controle voor het doel als bedoeld in artikel 7.1.c geldt dat slechts de e-mail en/of internetverkeersgegevens en inhoud van berichten wordt verwerkt.

8.6 In het kader van de controle voor het doel als bedoeld in artikel 7.1.d geldt dat:

a) de controle geheel geautomatiseerd plaatsvindt;

b) een gevonden besmet bericht/bestand op een aparte locatie bewaard wordt voor nader onderzoek en eventuele herstelwerkzaamheden.

8.7 In het kader van de controle voor het doel als bedoeld in artikel 7.1.d geldt dat slechts de
a) e-mailverkeersgegevens en inhoud (en bijlagen) van berichten met een verdachte inhoud worden gecontroleerd;
b) internetverkeersgegevens en inhoud van berichten met een verdachte inhoud worden gecontroleerd.

8.8 In het kader van de controle voor het doel als bedoeld in artikel 7.1.e geldt dat de controle van het e-mail- en internetverkeer beperkt blijft tot de verkeersgegevens.

8.9 In het kader van de controle voor het doel als bedoeld in artikel 7.1.e geldt dat slechts de
a) e-mailverkeersgegevens over tijd, hoeveelheid, omvang en dergelijke worden verwerkt;
b) internetverkeersgegevens over tijd en dergelijke worden verwerkt.

Artikel 9 Gebruik van social media

9.1 Onder social media wordt verstaan alle huidige en toekomstige online platformen waarbij de gebruikers de inhoud verzorgen.

9.2 Indien social media voor organisatiedoeleinden worden gebruikt dient dit – met het oog op de bescherming van persoonsgegevens - plaats te vinden conform het Privacyreglement.

9.3 Voor het overig gebruik geldt dat dit in eigen tijd dient plaats te vinden. Dat geldt ook voor het gebruik van social media door middel van smartphones of tablets.

9.4 Voor zover de gebruikers (medewerkers of derden) aan de organisatie verbonden zijn, geldt in algemene zin dat zich niet op social media zullen uitlaten op een wijze die schadelijk kan zijn voor Vogelaar.

Artikel 10 Richtlijnen voor het gebruik van social media

10.1 Voor zover de gebruiker op social media-uitingen doet die in relatie staan tot Vogelaar geeft hij steeds duidelijk aan in welke relatie (bijvoorbeeld: medewerker) hij staat tot Vogelaar.

10.2 De gebruiker plaatst op social media geen content met een onverantwoorde inhoud.

10.3 De gebruiker deelt op social media geen interne- of bedrijfsvertrouwelijke informatie over de organisatie.

10.4 De gebruiker deelt geen persoonsgegevens van medewerkers of anderszins betrokkenen waartoe hij uit hoofde van zijn functie toegang heeft.

10.5 De gebruiker laat zich op social media niet negatief of anderszins ongepast uit over de organisatie, over collega's, over medewerkers en/of over anderszins betrokkenen.

10.6 De gebruiker plaatst op social media niet zonder toestemming foto's of andere afbeeldingen van de organisatie en/of aan de organisatie verbonden medewerkers.

10.7 De gebruiker plaatst op social media geen content namens Vogelaar, tenzij hij daarvoor toestemming heeft gekregen.

10.8 In zijn algemeenheid geldt dat de gebruiker op social media geen content zal plaatsen of zich anderszins zal gedragen op een wijze die de organisatie schade kan toebrengen.

Artikel 11 Disciplinaire maatregelen

Indien door Vogelaar wordt vastgesteld dat een gebruiker onverantwoord gebruik heeft gemaakt van de ICT, kan Vogelaar - afhankelijk van de aard en de ernst van het onverantwoorde gebruik en de relatie van de gebruiker tot Vogelaar – maatregelen treffen, zoals een berisping, schorsing of ontslag.