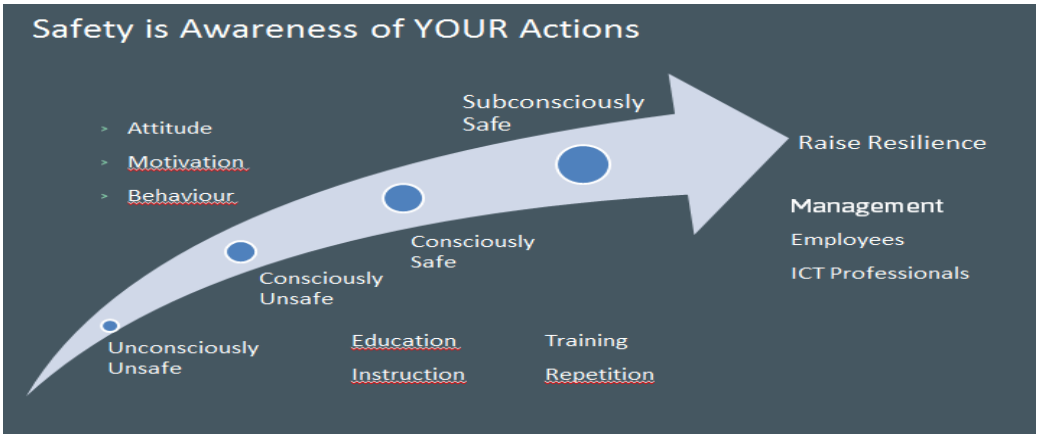
VEBON-NOVB Privacy Awareness Protocol

VEBON-NOVB
Postbus 840 | 2700 AV Zoetermeer
T 079 203 50 15
E info@vebon-novb.nl
I www.vebon-novb.nl

Inhoudsopgave

Inleiding

Iedere organisatie verwerkt informatie, vaak ook vertrouwelijke. Gegevens worden verzameld, (digitaal) vastgelegd of opgenomen in fysieke dossiers en indien noodzakelijk doorgegeven aan derden. Deze dagelijkse verwerking van vertrouwelijke gegevens betreft niet alleen persoonsgegevens van klanten, maar ook persoonsgegevens van medewerkers binnen uw organisatie.



Dit Privacy Awareness Protocol is opgesteld om:

1. praktische richtlijnen te geven voor de omgang met persoonsgegevens;
2. voor iedere werknemer de meldingsplicht en een beschrijving van de meldprocedure scherp te hebben.

VEBON-NOVB adviseert het management van alle leden dit Privacy Awareness Protocol minimaal 1x per jaar binnen de organisatie te bespreken met iedere werknemer, vast, flex, inleen of anderszins.

In aanvulling op de arbeidsovereenkomst en geldende richtlijnen binnen de onderneming wordt in dit Protocol aanbevolen te werken volgens de kernwaarden van de (brand)beveiligingsorganisatie inclusief de omgang met privacyvraagstukken.

Het Protocol bestaat uit twee delen:
1. Bedrijfskernwaarden
2. Een gedragscode: omgang met privacy

Deel 1

Bedrijfskernwaarden

Elke werknemer:

- is toegankelijk en aanspreekbaar;
- is vakbekwaam en weet wat zijn sterke punten zijn;
- behandelt iedere klant, collega en externe relatie met aandacht en respect;
- verplaatst zich in de belevingswereld van de ander en gaat in gesprek om duidelijk te krijgen wat nodig is;
- neemt verantwoordelijkheid voor het oplossen van problemen en mag daarbij altijd om hulp en advies vragen;
- geeft vertrouwen en ruimte voor verantwoordelijkheid;
- gaat collegiaal, veiligheidsbewust en oplossingsgericht te werk;
- komt zijn afspraken na en stelt het zelf aan de orde als dit onverhoopt niet lukt;
- neemt een onderzoekende houding aan en vraagt feedback op zijn gedrag en prestaties;
- vraagt zich af wat hij kan betekenen voor de organisatie en degenen met wie zij samenwerkt;
- weet wat in onze samenleving grensoverschrijdend is, handelt daarnaar en is daarop aanspreekbaar;
- signaleert in de eigen werkomgeving wat niet door de beugel kan én wat goed is maar verbeterd kan worden;
- kan – ook tegenover een kritische buitenstaander – uitleggen dat hij integer handelt;
- mag rekenen op een faire behandeling door zijn leidinggevende en zijn werkgever.

Mijn gedrag

	🔴	🟡	🟢
Ik heb een ‘clean desktop’: een leeg bureaublad			
Ik ken de gebruiksvoorwaarden en weet wat wel en niet toelaatbaar is op het netwerk			
Ik ken de regels over wachtwoordinstellingen en -gebruik			
Ik vergrendel altijd mijn scherm als ik mijn computer niet gebruik			
Ik schrijf wachtwoorden nooit op			
Ik meld alle incidenten aan de helpdesk			
Ik verbind mijn smartphone nooit met publieke WIFI			

🔴 Nooit

🟡 Soms

🟢 Altijd

Deel 2

Privacy

De Algemene Verordening Gegevensbescherming (AVG) zegt onder andere dat bedrijven en hun werknemers 'rechtmatig, behoorlijk en transparant' moeten zijn in hun omgang met persoonsgegevens. Iedere organisatie is daarmee verplicht iedere inbreuk op de beveiliging van persoonsgegevens te melden bij de Autoriteit Persoonsgegevens (AP), tenzij het niet waarschijnlijk is dat de inbreuk op de persoonsgegevens een risico inhoudt voor de rechten en vrijheden van natuurlijke personen.

Contactpersoon (beveiligingsfunctionaris)

Door werkgever is een beveiligingsfunctionaris of een Functionaris Gegevensbescherming (FG)* aangesteld en bekendgemaakt binnen de organisatie. Meldingen welke gemaakt dienen te worden conform de in dit document opgenomen items 'Omgang met persoonsgegevens' en 'meldingsplicht' dienen door de werknemer bij deze beveiligingsfunctionaris dan wel bij de direct leidinggevende te worden gedaan. De meldingsplicht bestaat uit – minimaal - een verzending per email én telefonisch contact.

Toelichting: Geef hier de naam van de beveiligingsfunctionaris of FG op of de naam van de afdelingsmanager/direct leidinggevende waaraan bericht wordt gestuurd.
* Een Beveiligingsfunctionaris of FG is kort gezegd een toezichthouder op de verwerking van persoonsgegevens.

Wie vrijwillig een FG aanstelt krijgt te maken met dezelfde regels die gelden voor een verplichte FG. Organisaties die dat een stap te ver vinden, kunnen ook een werknemer inzetten of een adviseur inhuren die zich met de bescherming van persoonsgegevens bezighoudt: de beveiligingsfunctionaris.

Nieuw in de AVG is dat de FG verplicht is voor:
1. De overheid;
2. Organisaties die op grote schaal verwerkingen doen en waarvan die verwerking ook de kernactiviteit van de organisatie is;
3. Organisaties die hoofdzakelijk belast zijn met het op grote schaal verwerken van bijzondere persoonsgegevens.

Wat te beschermen?

- ☐ Klantgegevens
- ☐ Accounts
- ☐ Ontwerpen/CAD tekeningen
- ☐ Intellectueel Eigendom (IE/OEM)
- ☐ Voorraad informatie
- ☐ Jaarcijfers
- ☐ Winst prognoses
- ☐ Reorganisatie plannen
- ☐ Gegevens werknemers/personeelsdossiers
- ☐ Tenders & contracten
- ☐ Telefoon- en e-mailadressen
- ☐ Logistieke processen
- ☐ CAD-CAM systemen
- ☐ Manufacturing
- ☐ Automatisering van processen
- ☐ ERP systemen
- ☐ Kasstroom
- ☐ Je merk
- ☐ Imago

Je reputatie!

Omgang met persoonsgegevens

1. Werknemers kunnen bij de uitvoering van hun werkzaamheden persoonsgegevens verwerken. Uitgangspunt is dat terughoudend wordt omgegaan met het verstrekken van persoonsgegevens aan collega's en aan derden. Verwerken van persoonsgegevens moet alleen functioneel zijn.

2. Het begrip “verwerken” omvat alle feitelijke handelingen met persoonsgegevens zoals: inzien, opslaan, wissen, aanpassen, doorsturen, afschermen.

3. Het begrip “persoonsgegeven” omvat ieder gegeven over een persoon die kan worden geïdentificeerd of identificeerbaar is. Veel voorkomende voorbeelden hiervan zijn naam, adres, e-mailadres, telefoonnummer, de inhoud van (e-mail)correspondentie, andere soorten elektronische berichten, foto’s, filmpjes, financiële gegevens, etc.

   Het begrip “bijzonder persoonsgegeven” omvat ieder gegeven dat zo gevoelig is dat de verwerking ervan iemands privacy ernstig kan beïnvloeden. Dergelijke gegevens mogen daarom alleen onder zeer strenge voorwaarden worden verwerkt.
   Voorbeelden van bijzondere persoonsgegevens zijn gegevens die iets zeggen over iemands gezondheid, ras, godsdienst, strafrechtelijk verleden of seksuele leven. Ook een lidmaatschap van een vakvereniging en het Burgerservicenummer (BSN) zijn bijzondere persoonsgegevens.

4. Werknemer zal:
   a) de persoonsgegevens geheimhouden;
   b) de persoonsgegevens uitsluitend verwerken voor zover dat noodzakelijk is voor het uitvoeren van de werkzaamheden, en deze niet op enige wijze voor eigen (privé) doeleinden verwerken;
   c) de persoonsgegevens niet aan enige derde buiten de organisatie van de werkgever beschikbaar maken, tenzij dat noodzakelijk is voor het uitvoeren van de werkzaamheden;
   d) de werkgever direct informeren als toch enige onbevoegde derde buiten de organisatie van de werkgever kennis neemt, of kan nemen van de persoonsgegevens;
   e) de door de werkgever aangegeven beveiligingsmaatregelen met betrekking tot de persoonsgegevens opvolgen;
   f) de door de werkgever aangegeven (overige) richtlijnen voor het verwerken van persoonsgegevens opvolgen.

Toelichting: Geef onder punt 4f aan welke andere richtlijnen en/of protocollen hier gelden en geef aan waar werknemer die kan vinden.

Kennis

Je ontvangt een e-mail van een onbekende afzender met een bijlage en/of een link om op te klikken. Wat doe je? ☐ Ik verwijder de e-mail direct ☐ Ik open de e-mail en antwoord de afzender dat ik SPAM niet op prijs stel ☐ Als het een grappige e-mail is stuur ik deze door naar een collega ☐ Als het aan mij is geadresseerd is het vast heel belangrijk ☐ Ik print de e-mail en geef het door aan de helpdesk	*Soms wordt er gevraagd om een nieuwe(re) versie van software te installeren op je PC. Wat doe je?* ☐ Dat kan ook een andere keer nog wel ☐ Ik klik het weg, ik heb andere dingen te doen ☐ Ik bevestig de software update ☐ Ik gebruik de software niet dus hoef ik het ook niet te updaten ☐ De huidige software werkt prima, dus ik hoef het niet te updaten
Phishing e-mail … ☐ Kan niet worden voorkomen ☐ Er kan niets gebeuren als het niet klikt ☐ Ik meld het bij de helpdesk en verwijder de e-mail daarna ☐ ICT zal het voorkomen ☐ Bevat altijd spelfouten	*Welke stelling over het wachtwoordbeleid van de organisatie waar je werkt is waar?* ☐ Het is moeilijk ☐ Er is geen wachtwoordbeleid ☐ Ik ken het beleid volledig ☐ Het is duidelijk en na te lezen ☐ Te veel regels om een wachtwoord te maken

Meldingsplicht

1. Werknemer is bekend met de verplichting diefstal en/of verlies van alle in het kader van de uitoefening van de functie door werkgever aan hem ter beschikking gestelde dan wel in het kader van de uitoefening van de functie te gebruiken informatie/gegevens of bescheiden/zaken direct na ontdekking te melden aan werkgever.
   Onder informatie/gegevens en bescheiden/zaken worden o.a. begrepen: documenten, telefoon, laptop, sleutels, passen, inloggegevens, al dan niet elektronische dragers van gegevens zoals USB-sticks, en externe harde schijven en andere zaken en/of bescheiden die op enige wijze betrekking hebben op de bedrijfsaangelegenheden van werkgever.

2. Werknemer is tevens verplicht om direct een melding te doen aan werkgever van de ontdekking van een actief virus, trojan of andere malware op een door werkgever aan werknemer ter beschikking gestelde of binnen het kader van de uitoefening van zijn functie door werknemer gebruikte computer, laptop, tablet, telefoon of ander apparaat.

3. Werknemer is voorts verplicht om direct een melding te doen aan werkgever van de ontdekking of bij een vermoeden dat op enige andere wijze persoonsgegevens onbedoeld openbaar zijn gemaakt.

4. Bij overtreding of niet-nakoming door werknemer van de genoemde verplichtingen kan dat leiden tot een officiële waarschuwing, berisping of een andere arbeidsrechtelijke maatregel.

* Met dank aan Sebyde, https://www.sebyde.nl/

VEBON-NOVB, Zoetermeer, april 2018