# Privacybeleid [NAAM ONDERNEMING]

## 1 - INLEIDING

Dit privacybeleid beschrijft op welke wijze de onderneming zorgdraagt voor een effectieve bescherming van de privacy van klanten, medewerkers en andere betrokkenen. Het verbindt de individuele documenten tot een geheel. Het privacybeleid is afgestemd op de eisen die door de Algemene Verordening Gegevensbescherming (AVG) worden gesteld.

**Evenwichtige risicogeörienteerde aanpak**

De belangen van de onderneming, van de betrokkene en van derden worden meegewogen in het privacybeleid en de uitvoering ervan. Maatregelen worden afgestemd op de privacyrisico's waarbij een balans wordt gevonden tussen de privacyrisico's en de kosten en inspanningen die maatregelen met zich meebrengen.

**Algemene beoordeling privacyrisico**

*Gevoeligheid gegevens*

Binnen de onderneming worden veelvuldig bijzondere/gevoelige persoonsgegevens verwerkt.
Binnen de onderneming wordt geen gebruik gemaakt van profilering.
Binnen de onderneming wordt geen gebruik gemaakt van (automatische) besluitvorming gebaseerd op profielen.
…….

*Omvang gegevensbestand*

De onderneming verwerkt persoonsgegevens van een aantal betrokkenen.

*Betrokkenen*

De betrokkenen zijn nooit een doelgroep die extra bescherming behoeft (zoals kinderen).

*Conclusie*

Op grond van het bovenstaande is het algemene privacyrisico binnen de onderneming in te schatten als relatief klein.

## 2 - SPELERS

**Management**

Binnen het management is Anne, eigenaar 'NJOY", verantwoordelijk voor de portefeuille privacy. Jaarlijks staat de bespreking van de effectiviteit van het privacybeleid op de agenda van het management.

**Privacyverantwoordelijke**

Binnen de onderneming is Babette aangewezen als privacyverantwoordelijke. Deze persoon houdt toezicht op de uitvoering van het privacybeleid en zorgt voor de evaluatie en ontwikkeling van het privacybeleid. Deze persoon is aanspreekpunt voor privacygerelateerde vragen en verzoeken van medewerkers en van betrokkenen. Deze persoon is bereikbaar via njoy-tp@outlook.com.

**Proceseigenaar**

Medewerkers die verantwoordelijk zijn voor een proces waarbij persoonsgegevens worden verwerkt zijn verantwoordelijk voor de waarborging van de privacy binnen dat proces. Hierdoor komt de waarborging van privacy zo dicht mogelijk bij de medewerkers te liggen die de persoonsgegevens verwerken. De procesverantwoordelijke medewerkers worden getraind zodat zij deze taak met de nodige kennis kunnen uitvoeren.

**Medewerkers**
Alle medewerkers hebben een verantwoordelijkheid om correct met persoonsgegevens en de software en hardware waarop deze staan opgeslagen om te gaan. De medewerkers zijn geïnformeerd en indien nodig getraind over hoe dient te worden omgegaan met persoonsgegevens binnen de onderneming.

**Adviseur – privacyexpert**
Voor praktische of juridische vragenstukken over privacy kan via de privacyverantwoordelijke contact worden opgenomen met Kompas Juristen (tel: 020-7552416 / mail: info@kompasjuristen.nl).

**Betrokkenen**
De natuurlijke personen van wie de persoonsgegevens worden verzameld zijn de betrokkenen. De belangrijkste groepen betrokkenen binnen de onderneming zijn de klanten, de potentiële klanten en de medewerkers.

## 3 - PRIVACYCULTUUR

**Trainen & informeren van medewerkers**
Medewerkers worden geïnformeerd over het privacybeleid van de onderneming en over het waarborgen van privacy in relatie tot de persoonsgegevens waar de medewerkers mee in aanraking komen. Medewerkers worden geïnformeerd over de rechten die betrokkenen hebben en hoe deze rechten specifiek binnen de onderneming kunnen worden uitgeoefend. Medewerkers die verantwoordelijk zijn voor processen waarbij persoonsgegevens worden verwerkt, worden getraind op welke wijze zij deze processen AVG-conform en privacyvriendelijk kunnen inrichten.

**Privacy meewegen in de besluitvorming**
Bij de aanschaf van nieuwe software, clouddiensten of hardware wordt de waarborging van privacy als factor meegewogen in het aankoop- en ontwikkelproces door onder meer 'privacy by design' en de beveiliging van persoonsgegevens te beoordelen.

**Melding door medewerkers**
Medewerkers worden gestimuleerd om verbeteringen met betrekking tot privacy aan te dragen. Jaarlijks krijgen medewerkers hiertoe een oproep.

## 4 – ONDERDELEN VAN HET PRIVACYBELEID

Om de privacy van betrokkenen te waarborgen en om te voldoen aan de eisen de die AVG stelt aan de verwerking van persoonsgegevens worden de navolgende punten binnen de onderneming in acht genomen.

**Beoordeling en aanpassing van processen (privacy by design & default)**
Bij de aanpassing van processen en in het bijzonder de aanschaf of ontwikkeling van nieuwe IT systemen wordt er een verantwoordelijke aangesteld die een beoordeling maakt van de privacyaspecten en passende maatregelen implementeert ter waarborging van de privacy. Deze beoordeling wordt gegoten in de vorm van een privacy impact assessment (PIA) indien de privacyrisico's voor de betrokkenen waarschijnlijk groot zijn. Bij de inrichting van processen worden enkel de noodzakelijke gegevens verwerkt en deze gegevens worden niet verder in de onderneming verwerkt dan nodig voor de doeleinden waarvoor deze zijn verkregen of doelen die daarmee verenigbaar zijn (dataminimalisatie).Bij de inrichting van processen worden privacybevorderende maatregelen genomen. Bij de inrichting van processen wordt beoordeeld op welke wijze niet meer noodzakelijke data effectief en efficiënt kan worden verwijderd.

**Verwerkingsregister**
Binnen de onderneming is er op een centraal punt een register met daarin opgenomen welke persoonsgegevens binnen welke processen worden verwerkt. Het verwerkingsregister is opgesteld per proces waarin in ieder geval is opgenomen:

- de categorieën persoonsgegevens,
- de categorieën betrokkenen
- de doeleinden van de verwerking,
- de grondslag, het gerechtvaardigd belang indien dit de grondslag vormt,
- de bewaartermijnen,
- met welke partijen buiten de onderneming de persoonsgegevens worden gedeeld.
- of persoonsgegevens worden doorgegeven naar landen buiten de EU en zo ja welke landen. (Dit ziet voornamelijk op dataopslag buiten de EU door verwerkers. Doorgifte aan reisdienstverleners wordt niet opgenomen in het register.)

De procesverantwoordelijke bezit zelf ook een versie van het verwerkingsregister voor zijn proces.

**Bewaartermijnen en verwijderen van gegevens**
Voor ieder proces binnen de onderneming waarbij persoonsgegevens worden verzameld, bepaalt de procesverantwoordelijke de bewaartermijnen van de verzamelde gegevens (bewaren mag niet langer dan noodzakelijk voor de doeleinden waarvoor de persoonsgegevens zijn verkregen). De procesverantwoordelijke stelt een protocol op voor het proces hoe de niet-noodzakelijke persoonsgegevens c.q. persoonsgegevens waarvan de bewaartermijn is verstreken zo efficiënt mogelijk worden verwijderd. Het wordt gestimuleerd om dit geautomatiseerd of semi-geautomatiseerd te doen. Bij de aanschaf of ontwikkeling van nieuwe IT-systemen wordt rekening gehouden of het systeem is ingericht om efficiënt niet meer noodzakelijke persoonsgegevens te verwijderen.

**Beveiliging**
Er worden passende technische en organisatorische beveiligingsmaatregelen genomen, rekening houdend met de stand van de techniek en de uitvoeringskosten, om een op het risico afgestemd beveiligingsniveau te waarborgen.

Onder meer de beveiligingsmaatregelen uit de volgende bronnen worden overwogen:

- Richtsnoeren beveiliging persoonsgegevens (website Autoriteit Persoonsgegevens)
- Code voor informatiebeveiliging - ISO 27002
- Relevante adviezen van het Nationaal Cyber Security Centrum

Voor zover gebruik wordt gemaakt van webapplicaties eveneens:

- OWASP top 10 (actuele versie)
- ICT beveiligingsrichtlijn voor webapplicaties (website Nationaal Cyber Security Centrum) (actuele versie)

De genomen beveiligingsmaatregelen zijn gedocumenteerd in bijlage I ‘Databeveiligingsmaatregelen’. Jaarlijks wordt de effectiviteit van de beveiligingsmaatregelen geëvalueerd.

Een beveiligingstest geschiedt jaarlijks voor de website en e-mail via www.internet.nl

**Beoordeling verwerkers en verwerkersovereenkomsten**
Ingeschakelde verwerkers dienen voldoende garantie te bieden dat zij voldoen aan de AVG en de persoonsgegevens passend beveiligen. Het aansluiten bij een overeenkomstig de AVG goedgekeurde gedragscode (art. 40 AVG) of een goedgekeurd certificeringsmechanisme (art. 42 AVG) kan worden gebruikt als element om aan te tonen dat voldoende garanties worden geboden. Met verwerkers wordt een adequate verwerkersovereenkomst gesloten.

**Telewerken & BYOD**
Voor medewerkers die buiten het terrein van de onderneming (‘telewerken’) en/of op eigen apparatuur (‘Bring Your Own Device’)(in functie) persoonsgegevens verwerken geldt het beleid ‘Telewerken & BYOD’
Medewerkers die buiten het terrein van de onderneming (in functie) persoonsgegevens verwerken hebben het beleid telewerken ontvangen en gelezen/ondertekend.

Medewerkers die op eigen apparatuur, zoals laptop, tablet, telefoon,…, (in functie) persoonsgegevens verwerken hebben het beleid 'Telewerken& BYOD' ontvangen en gelezen/ondertekend.

**Overeenkomsten met medewerkers en vrijwilligers**
Met medewerkers is (in de arbeidsovereenkomst) een geheimhoudingsbeding overeengekomen. In het beding is opgenomen dat de medewerker is gehouden tot geheimhouding van persoonsgegevens waar de medewerker uit hoofde van de arbeidsrelatie kennis van heeft. De verplichting dient voort te duren na het einde van de arbeidsovereenkomst. Voor zover de onderneming gebruik maakt van vrijwilligers, stagiaires, e.d. wordt een geheimhoudingsverklaring van gelijke strekking overeengekomen.

**Rechten van betrokkenen**
Indien een betrokkene zijn recht conform de AVG wil uitoefenen kan de betrokkene hiertoe schriftelijk een verzoek indienen. Dit verzoek mag worden gericht aan de privacyverantwoordelijke. Indien de betrokkene op andere wijze een verzoek indient wordt het verzoek doorgestuurd aan de privacyverantwoordelijke. De privacyverantwoordelijke neemt zo nodig contact op met de betrokkene.

De privacyverantwoordelijke coördineert de afhandeling van het verzoek en controleert de naleving van het verzoek.

**Informatie van betrokkenen**
Per proces is de toepasselijkheid en deugdelijkheid van de privacyverklaring gecontroleerd. De betrokkenen worden op de volgende wijze geïnformeerd:

- Klanten > privacyverklaring website
- Websitebezoekers > Cookietekst op de landingspagina + privacyverklaring website
- Medewerkers . privacyverklaring personeelshandboek
- …

**Klachten van betrokkenen**
In de privacyverklaring is een intern klachtprotocol opgenomen. Hierin staat beschreven dat betrokkenen zich met klachten kunnen wenden tot de privacyverantwoordelijke. De privacyverantwoordelijke zal de ontvangst van de klacht onverwijld bevestigen en binnen 1 maand inhoudelijk reageren.

**Beveiligingsincidenten & datalekken**
Zo veel mogelijk handelingen in IT systemen worden gelogd om te kunnen achterhalen wie toegang heeft gehad tot welke persoonsgegevens, of onrechtmatige toegang is verkregen tot persoonsgegevens en of hier pogingen toe zijn ondernomen.

Er geldt een intern protocol datalekken. Bij alle medewerkers is het protocol datalekken bekend. Datalekken en ook beveiligingsincidenten zonder gevolgen worden geëvalueerd en geregistreerd door de privacyverantwoordelijke.

**PIA**
De privacyverantwoordelijke voert – al dan niet met externe hulp - een Privacy Impact Assessment (PIA) uit indien de verwerking:

- gelet op de aard, omvang, context en doeleinden
- waarschijnlijk

- een hoog privacy risico oplevert voor de betrokkenen

Dat is in ieder geval zo als:

- systematisch en uitvoerig persoonlijke aspecten geautomatiseerd worden geëvalueerd (waaronder profileren),
- op grote schaal bijzondere persoonsgegevens worden verwerkt,
- op grote schaal en systematisch mensen worden gevolgd in een publiek toegankelijk gebied.

**5 - AANTOONBAARHEID**

**Documentatie**
De volgende geactualiseerde documenten zijn centraal opgeslagen in de map privacy:

- Het privacybeleid inclusief beveiligingsbeleid
- De verwerkingsregisters per proces
- Verwijderingsprotocollen per proces
- Een kopie van de privacyverklaringen
- Een kopie van de verwerkersovereenkomsten
- Het beleid 'Telewerken en BYOD'
- Het protocol datalekken
- Authorisatieschema (welke medewerker heeft toegang tot welke gegevens)
- IT-beheerdocument (wie heeft welk mobiele apparaat)

**Effectiviteit van het beleid/self-assessment**
De effectiviteit van het privacy wordt gemeten met een self-assessment aan de hand van de parameters actualiteit en volledigheid voor de volgende punten:

- Worden per proces niet meer gegevens dan noodzakelijk verzameld?
- Zijn de verwerkingsregisters voor alle processen actueel en volledig?
- Zijn de beveiligingsmaatregelen actueel en volledig?
    - beveiligingstest website en e-mail via www.internet.nl
- Zijn met alle medewerkers/stagiaires/e.d. geheimhoudingsovereenkomsten getekend?
- Zijn de persoonsgegevens waarvan de bewaartermijn is overschreden verwijderd?
- Zijn de privacyverklaringen voor alle processen actueel en volledig?
- Zijn alle verwerkers beoordeeld op de factor privacy & databeveiliging en zijn er adequate verwerkersovereenkomsten gesloten?

Privacy-scoreboard

| | Score actualiteit | Score volledigheid |
|---|---|---|
| Processen voldoen aan privacy by design&default (o.a. dataminimalisatie) | | |
| Verwerkingsregister | | |
| IT - beveiligingsmaatregelen | | |
| Organisatorische beveiling | | |
| Geheimhouding | | |
| Verwijdering van gegevens | | |
| Privacyverklaring | | |
| Relatie met verwerkers | | |

De meting geschiedt per proces waarbij de procesverantwoordelijke de beoordeling uitvoert en zo nodig overlegt met de privacyverantwoordelijke.
Aanvullend worden de beveiligingsincidenten en de privacygerelateerde klachten geëvalueerd.

**Evaluatie en continuïteit**
Het privacybeleid en de uitvoeringsmaatregelen worden op regelmatige basis maar in ieder geval jaarlijks beoordeeld en aangepast waar nodig (plan-do-check-act cyclus).
Indien processen tussentijds veranderen wordt de factor privacy meegewogen in de aanpassing en worden het beleid en de documentatie van privacymaatregelen aangepast op de nieuwe situatie.

## 6 – HANDIGE WEBSITES

De tekst van de Algemene verordening gegevensbescherming is onder meer na te lezen op www.verordeninggegevensbescherming.nl

Op de website van de Autoriteit Persoonsgegevens ( www.autoriteitpersoonsgegevens.nl ) staan veel adviezen.

Op de website van het Nationaal Cyber Security Centrum staan veel praktische adviezen over de beveiliging ( www.ncsc.nl )

**BIJLAGE I - Databeveiligingsmaatregelen**

**Fysieke toegang**

- De toegang tot het kantoor is fysiek beperkt tot personen die daartoe bevoegd zijn (bijvoorbeeld door middel van een sleutel/pasje/code, al dan niet aangevuld met toegangsregistratie).
- Er is een adequaat sleutel-, toegangscode- en alarmcodebeheer.
- De toegang tot de ruimtes waar (digitale media met) persoonsgegevens staan opgeslagen is fysiek beperkt tot personen die daartoe bevoegd zijn. (Bijvoorbeeld door middel van slot & sleutel.)
- Op papier gedrukte gevoelige of bijzondere persoonsgegevens (zoals personeelsgegevens) staan in een afgesloten kast. Overige persoonsgegevens staan in een ruimte die kan worden afgesloten en is afgesloten indien er niemand aanwezig is.
- Er geldt een clear desk en clear screen policy.

**Toegangsrechten/autorisatie van medewerkers**

- Toegang tot mappen op de harde schijf/server is beperkt op een need to know basis.
- Toegang tot IT-platformen en onderdelen daarvan is beperkt op een need to know basis.
- Toegang tot personeelsgegevens is beperkt op een need to know basis.
- Toegang tot bijzondere of gevoelige persoonsgegevens is beperkt op een need to know basis (denk aan medische gegevens).
- Toegangsrechten van gebruikers worden adequaat beheerd en geactualiseerd.
- Toegangsrechten worden aangepast bij een functiewissel/taakwissel.
- Toegangsrechten worden op de dag dat de arbeidsovereenkomst c.q. de actieve arbeid van een medewerker of vrijwilliger eindigt ingetrokken.

**Netwerkbeveiliging**

- Er is adequate beveiliging bij toegang tot het netwerk waaronder identificatie van vertrouwde apparaten.
- Er is adequate beveiliging bij toegang tot het netwerk waaronder een lijst van ‘geblokkeerde’ landen van waaruit geen toegang tot het netwerk mogelijk is of een lijst van landen van waaruit wel toegang mogelijk is.

**Eigen wifi-netwerk**

- Het wifi-wachtwoord van het bedrijfsnetwerk is enkel bekend bij de medewerkers en bevoegde personen en het wordt niet gedeeld met gasten.

**Beheer van IT-middelen**

- Er is een overzicht van IT-middelen waarop persoonsgegevens worden verwerkt (computers, laptops, tablets, telefoons, printer met dataopslag, USB-sticks, etc.).
- Er is adequaat beheer van de IT-middelen. Er is te allen tijde bekend bij wie de IT-middelen zijn.
- IT-middelen met persoonsgegevens mogen enkel worden meegenomen buiten het terrein indien hier goedkeuring van verantwoordelijke voor de IT-middelen voor is.

**Toegang tot IT**

- De toegang tot desktopcomputers is beveiligd met een adequaat wachtwoord of ander beveiligingsmechanisme.
- De toegang tot laptops is beveiligd met een adequaat wachtwoord of ander beveiligingsmechanisme.

- ➢ De toegang tot andere apparaten (in het bijzonder tablets/telefoons) is beveiligd met een adequaat wachtwoord of ander beveiligingsmechanisme.
- ➢ Er is een session time out/automatische schermblokkering ingesteld bij niet-gebruik van de apparaten (3-5 minuten).
- Het beeldscherm wordt bij verlaten van de werkplek geblokkeerd. (Sneltoets: "Windowstoets + L" (L van lunch).)

**Wachtwoorden**

- Er zijn afspraken over wachtwoordvereisten en wachtwoordbeheer.
- ➢ Er worden geen eenvoudig te raden wachtwoorden gebruikt.
- ➢ De wachtwoorden worden niet opschreven, tenzij dit geschiedt in een beveiligde (digitale) wachtwoordkluis.
- ➢ Wachtwoorden/inloggegevens worden niet automatisch opgeslagen.
- ➢ Wachtwoorden worden niet gedeeld. Ook niet met familie/collega's.
- ➢ Wachtwoorden worden jaarlijks veranderd.
- Er zijn automatische controles/procedures die leiden tot het instellen van een sterk wachtwoord.
- ➢ Een sterk wachtwoord bestaat uit minimaal 8 tekens, waarvan tenminste: 1 hoofdletter, een kleine letter, een cijfer en een speciaal teken (Stand der techniek december 2017).
- ➢ Bij meer dan 3 foutieve inlogpogingen wordt automatisch de toegang – gedurende een periode – ontzegd.
- Bij een foute inlogpoging wordt enkel vermeld dat er sprake is van een foutieve combinatie van inloggegevens. Er wordt niet vermeld of de gebruikersnaam actief is.
- Inlogactiviteiten worden gelogd.
- Wachtwoorden (in het bijzonder voor externe toegang tot het netwerk) worden gecodeerd verstuurd.
- Het bovenstaande geldt voor alle inlogprocedures.

**Twee factoren authenticatie**

- Voor de beveiliging van zeer gevoelige data is meervoudige authenticatie gewenst (Naast een gebruikersnaam en een wachtwoord moet dan bijvoorbeeld ook een vingerafdruk of code ingevoerd worden, die je via sms of via een bijbehorende smartphone-app ontvangt).

**Logging**

- Er is een log per IT-platform van gebruikersactiviteiten. (Hiermee kun je onrechtmatige verwerking achterhalen.)

**Opslag**

- Persoonsgegevens worden beveiligd opgeslagen.
- ➢ Er zijn heldere afspraken met medewerkers en vrijwilligers over de plaats waarop persoonsgegevens worden opgeslagen (netwerkmappen, lokale mappen, e-mails, andere plaatsen).
- Gebruik beveiliging op netwerkmappen en waar nodig ook beveiliging op bestanden op het netwerk.
- Bijzondere en gevoelige persoonsgegevens worden 'versleuteld' opgeslagen.
- Bijzondere en gevoelige persoonsgegevens worden waar mogelijk 'gepseudonimiseerd' opgeslagen.
- Er is overzicht op welke plaatsen de data fysiek staat opgeslagen.
- De server is adequaat beveiligd.
- Indien de server wordt gedeeld met een andere organisatie dan zijn er heldere afspraken over servergebruik en veilige toegang tot de server.

**Verwijdering van persoonsgegevens**

- Er zijn bewaartermijnen bepaald en er zijn – al dan niet geautomatiseerde - procedures waardoor de persoonsgegevens die de bewaartermijn overschrijden worden verwijderd.
- IT-hardware en USB-sticks worden op adequate wijze gewist of vernietigd, wanneer zij niet meer worden gebruik.
- De papieren versies van (gevoelige of bijzondere) persoonsgegevens worden adequaat vernietigd (bijvoorbeeld met een papierversnipperaar met DIN-vernietigingsnorm categorie 3 of 4).

**Dataverkeer**

- Bij het verkrijgen van persoonsgegevens via het internet wordt gebruik gemaakt van beveiligde protocollen zoals een ssl-certificaat (https).
- Lijsten met persoonsgegevens worden beveiligd verstuurd. (In Ms Excel, Ms Word en pdf kan je eenvoudig een bestand beveiligen met een wachtwoord.) Idealiter stuur je het wachtwoord via een apart medium (SMS/telefoon/brief)
- Bijzondere of gevoelige persoonsgegevens worden beveiligd en bij voorkeur versleuteld verzonden.
- ➢ Er worden enkel USB sticks met toegangsbeveiliging en/of versleuteling gebruikt voor de opslag van persoonsgegevens (alle onbeveiligde USB-sticks worden ingeleverd en vervangen).

**Website**

- De website is ondertekend met een geldige DNSSEC handtekening. (Dit beschermt tegen manipulatie van de domeinnaam.)
- ➢ HTTPS is beschikbaar én wordt afgedwongen.
- HTST is beschikbaar.
- De webserver ondersteunt alleen voldoende beveiligde TLS.
- De website beschikt over een geldig webcertificaat en de vertrouwensketen van het webcertificaat is goed.
- De websitedomein bevat een TLSA record voor Dane.

**E-mail**

- DNSSEC is aanwezig en geldig voor het e-maildomein en de mailserver (authenticatie van e-mail)
- DKIM is actief (bepaling authenticiteit e-mail)
- SPF is actief (whitelist van mailservers van waaruit jouw mails mogen worden verstuurd)
- Actieve DMARC Policy (beleid omgang niet-authentieke e-mails.)
- STARTTLS is actief
- Er is een geldig mailservercertificaat en de vertrouwensketen van het certificaat is goed.
- De e-mail bevat een TLSA record voor Dane.

**Software**

- De laatste versie van het besturingsprogramma is geïnstalleerd op apparaten.
- ➢ Gebruikte software is voorzien van de laatste updates.
- Er kan geen software op computers van medewerkers worden opgeslagen zonder toestemming van de IT-beheerder. Op bedrijfsmiddelen mag enkel de IT-beheerder software downloaden of installeren. Voor andere gebruikers dient dit technisch onmogelijk te zijn.

**Malware/virussen**

- Er is een up to date firewall en virusscanner op alle IT-middelen geïnstalleerd.
- Er is een adequate firewall en virusbescherming op het netwerk geïnstalleerd.

- Medewerkers zijn verplicht USB-sticks en andere verwijderbare media die worden aangesloten op het netwerk eerst te scannen op virussen of dit gebeurt automatisch.
- ➢ Inkomende e-mails worden automatisch gecontroleerd op virussen, trojans en andere malware.

**Back-up**

- ➢ Er is een regelmatige back-up van de gegevens.
- De back-up omvat alle persoonsgegevens. Niet alleen netwerkmappen op de server en e-mails, maar ook lokale mappen voor zover daar persoonsgegevens staan opgeslagen die niet ook op de server staan. (Dit is enkel haalbaar indien er heldere afspraken zijn over waar data wordt opgeslagen).
- De back-up wordt jaarlijks getest (recovery test).
- ➢ De back-up is beveiligd.

**Mobiele apparaten (laptops/tablets/telefoons)**

- Mobiele apparaten zijn fysiek beveiligd indien er geen toezicht is (achter slot en grendel).
- ➢ Mobiele apparaten zijn technisch beveiligd (wachtwoord, firewall, antivirus, automatisch sessie beëindigen, etc.).
- ➢ Er is VPN geïnstalleerd op mobiele apparaten (ten behoeve van veilig wifigebruik).
- Er worden zo min mogelijk persoonsgegevens opgeslagen op mobiele apparaten.
- Opslag geschiedt centraal op de netwerkserver via een virtuele desktoptoegang en niet op het apparaat.
- Mobiele apparaten kunnen op afstand onbruikbaar worden gemaakt of de gegevens kunnen op afstand worden verwijderd.
- De harde schijf, SSD of andere opslag van mobiele apparaten is beveiligd/versleuteld zodat deze bij verlies niet toegankelijk of uitleesbaar is. (Beveiliging van het mobiele apparaat met een wachtwoord is dus mogelijk onvoldoende).
- Indien persoonsgegevens op mobiele apparaten worden opgeslagen wordt er ook een back-up van de harde schijf/SSD gemaakt.
- Er is een effectief beleid hoe medewerkers en vrijwilligers met mobiele apparaten dienen om te gaan.

**Telewerken (alle werkzaamheden buiten kantoor)**

- Inloggegevens/wachtwoorden worden gecodeerd verstuurd.
- ➢ Er wordt geen gebruik gemaakt van openbare wifi, tenzij adequate beveiligingsmaatregelen zijn genomen. Het beste is een eigen mobiele hotspot via de eigen mobiele telefoon. Is dit niet mogelijk, zorg dan dat je navraagt bij een bedrijf wat de correcte openbare wifi is én maak een beveiligde verbinding met VPN (met name in buitenlandse bars en hotels van groot belang!).
- ➢ Houdt bij openbare werkplekken de apparaten te allen tijde onder toezicht (ook bij korte pauzes).
- Er is een beleid voor telewerken.

**Printer**

- Het is mogelijk om gevoelige gegevens zoals personeelsgegevens op een beveiligde of apart toegankelijke printer te printen.
- Het is beleid om gevoelige gegevens te verwijderen van het printergeheugen.

**Webapplicaties**

- Zorg dat webapplicaties adequaat beveiligd zijn. Richtlijnen zijn onder meer de OWASP top 10 en de uitgave beveiliging webapplicaties van het National Cyber Security Centrum.
- Doorgaans worden webapplicaties van derden gebruik. Zorg dat bij verwerking door deze verwerkers ook adequate beveiligingsmaatregelen worden genomen door de verwerkers. De afspraken hierover liggen vast in de verwerkersovereenkomst.

**Gebruik privéapparatuur**

- Er zijn heldere afspraken over gebruik van privéapparatuur (hier wordt voor getekend).
- Het gebruikte apparaat wordt aangemeld.
- De meest recente versie van antivirussoftware is geïnstalleerd
- Er is een up to date firewall geïnstalleerd
- Het besturingsprogramma en gebruikte software zijn volledig geüpdatet.
- Enkel de noodzakelijke persoonsgegevens worden opgeslagen.
- Deze persoonsgegevens worden zo spoedig mogelijk – duurzaam – verwijderd
- Er worden geen bijzondere of gevoelige persoonsgegevens opgeslagen.
- Opslag geschiedt in een met een wachtwoord beveiligde map en de mapinhoud is niet vindbaar via de algemene searchbalk.

**Kennis en bewustwording**

- Bij medewerkers is de nodige kennis aanwezig om adequaat met persoonsgegevens en IT-middelen om te gaan.
- In de arbeidsovereenkomst van medewerkers is een geheimhoudingsbepaling opgenomen (die ook geldt na einde dienstverband).
- Bij vrijwilligers is de nodige kennis aanwezig om adequaat met persoonsgegevens en IT-middelen om te gaan.
- Laat alle vrijwilligers een geheimhoudingsverklaring tekenen, zodat men zich bewust is van de risico's en hun rol daarin.

**Evaluatie en ontwikkeling**

- Test en evalueer jaarlijks de effectiviteit van het beleid, de maatregelen en de beveiliging.
- Blijf up to date van actuele (technische) beveiligingsmaatregelen ( www.ncsc.nl ).
- Voer de nodige verbeteringen door op basis van de evaluatie en externe ontwikkelingen.