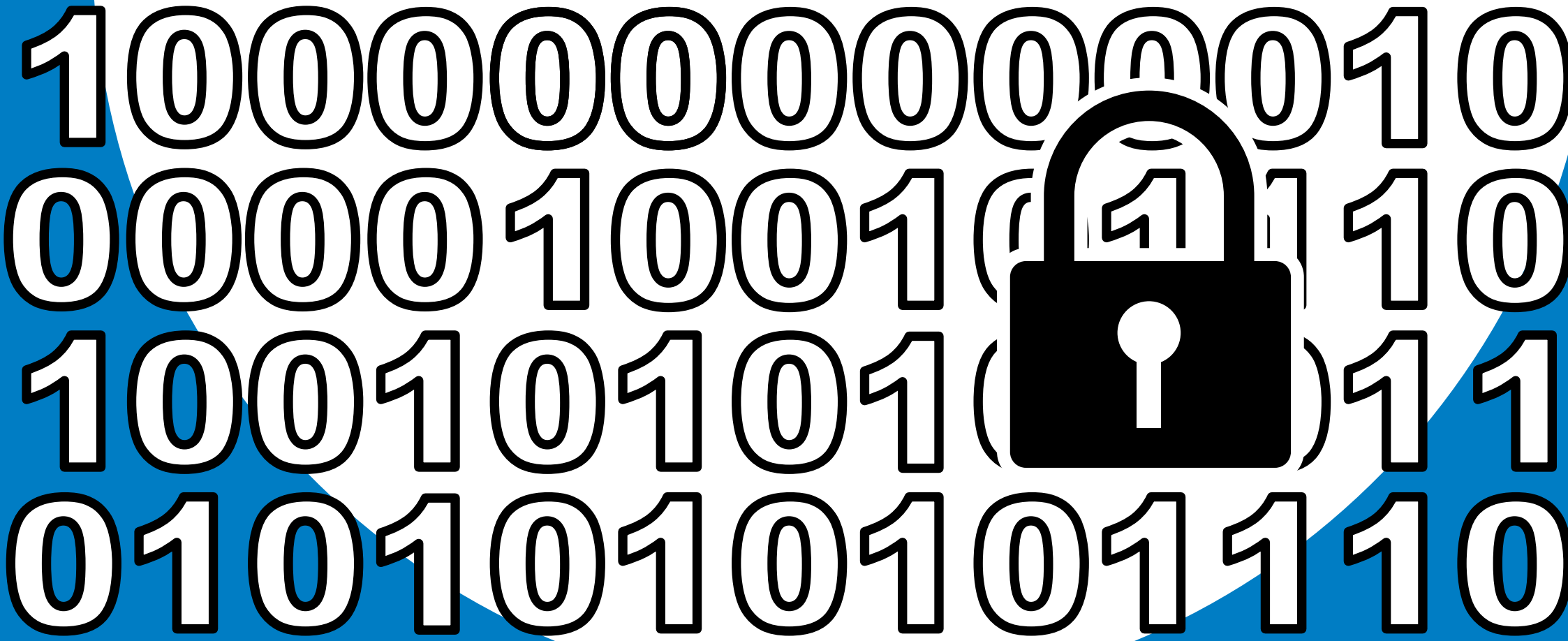
MOA Richtlijn Data Beveiliging

Versie 2018



EXPERTISE CENTER FOR
MARKETING-INSIGHTS, ONDERZOEK & ANALYTICS

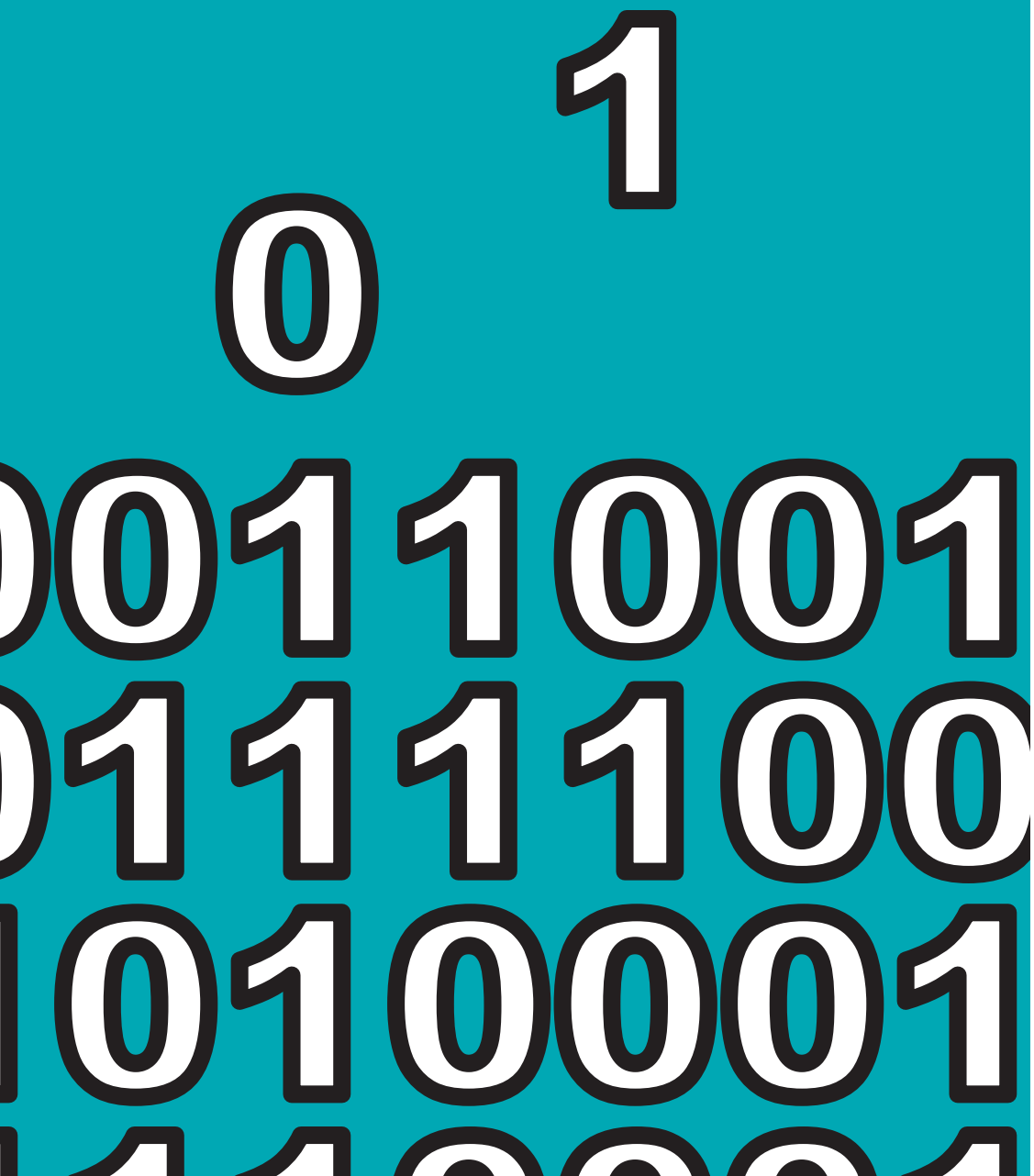
MOA Richtlijn Beveiliging

met MOA model Verwerkersovereenkomst en gebaseerd
op de Algemene Verordening Gegevensbescherming (AVG)
die op 25 mei 2018 in werking treedt

Februari 2018

Inhoudsopgave

MOA Richtlijn Data Beveiliging



Inleiding

Databeveiliging is een onderwerp dat momenteel sterk in de belangstelling staat van onderzoeksorganisaties en hun opdrachtgevers. In dit document wordt in hoofdlijnen beschreven aan welke minimale beveiligingseisen een onderzoeksorganisatie moet voldoen en hoe dit niveau bereikt kan worden.
Alle gebruikers van (rand)apparatuur, zoals PCs, laptops, tablets, smartphones etc., moeten gebruik maken van alle aan hen ter beschikking gestelde praktische middelen die zorgen voor een veilige bewaring van gegevens (bijvoorbeeld wachtwoordbeleid, fysieke beveiligings- en controlemiddelen, etc.)

Het beveiligingsbeleid beperkt zich niet tot persoonsgegevens maar heeft ook betrekking op de bedrijfsgegevens van de opdrachtgevers van onderzoeksorganisaties, zoals onderzoeksrapportages, etc.

Dit document geeft antwoord op basisvragen op het gebied van informatiebeveiligingsbeleid en daaraan gerelateerde zaken. Het is tevens gericht op het verhogen van de bewustwording van de noodzaak tot informatiebeveiliging bij alle medewerkers in dienst van een onderzoeksorganisatie en de door de organisatie ingehuurde externe krachten. Voorts geeft dit document een verdere (concretere) invulling van de in ISO 20252:2012 geformuleerde eisen met betrekking tot databeveiliging.

Het is van groot belang dat organisaties (opdrachtgevers) en consumenten (respondenten) erop kunnen vertrouwen dat onderzoeksorganisaties goed omgaan met informatie, waaronder persoonsgegevens. Verlies, ongewenste openbaarheid en/of ongeautoriseerd gebruik van informatie kan de positie van een onderzoeksorganisatie negatief beïnvloeden. Bovendien bevat de informatie die verwerkt wordt in de systemen van een onderzoeksorganisatie, inclusief de rapportage daarvan, veelal waardevolle en/of gevoelige informatie over de opdrachtgever en de respondenten. Daarmee heeft de onderzoeksorganisatie de verplichting om integer met deze informatie om te gaan en bescherming te bieden tegen onrechtmatige verwerking en verlies.

Onderzoeksorganisaties, die bedrijfslid zijn van de MOA, moeten deze MOA Richtlijn Data Beveiliging, of een gelijksoortig protocol, in hun organisatie als uitvloeisel van hun lidmaatschap implementeren. Het niet of niet volledig implementeren van deze MOA Richtlijn Data Beveiliging, of een ander gelijksoortig protocol, kan leiden tot een eenzijdige opzegging van het lidmaatschap van de MOA.

Een algemene ‘quicklist’

Voordat meer beleidsmatig wordt ingegaan op databeveiliging, wordt aanbevolen om een aantal minimaal te nemen maatregelen te beschrijven via onderstaande quicklist:

1. Beperk de toegang tot de gegevens (intern en extern)
2. Beperk de opslag van identificerende gegevens
3. Verwerk niet meer persoonsgegevens dan noodzakelijk en zorg dat deze juist en correct zijn
4. Voorkom datalekken
5. Sla bijzondere of in de context als zeer gevoelig ervaren gegevens altijd geëncrypteerd op
6. Sluit met de opdrachtgever indien zijn/haar persoonsgegevens worden verwerkt door de onderzoeksorganisatie een Verwerkersovereenkomst
7. Zorg dat de onderzoeksorganisatie weet waar randapparatuur zich bevindt en beveilig deze tegen onrechtmatig gebruik of verlies van persoonsgegevens

Algemene principes inzake gegevensbeveiliging

Het volgen van de hiervoor genoemde quicklist is een eerste aanzet tot beveiliging van data. Om tot een meer afgewogen en integraal beveiligingsbeleid te komen zijn vier pijlers van belang:

1. **Confidentiality (vertrouwelijkheid)** – Gegevens mogen niet openbaar gemaakt worden aan ongeautoriseerde personen, zowel binnen als buiten de onderzoeksorganisatie. De onderzoeksorganisatie dient te waarborgen dat informatie alleen toegankelijk is voor degenen die hiertoe geautoriseerd zijn. Ongeautoriseerde vrijgave van gegevens en informatie kan leiden tot aanzienlijke financiële schade en/of nadeel;

2. **Integrity (integriteit)** – Gegevens die met zorg en precisie zijn verzameld en verwerkt, verstrekken betrouwbare informatie over de bedrijfsactiviteiten van de onderzoeksorganisatie en haar opdrachtgevers. Deze informatie mag niet worden gemodificeerd/gecorrumpeerd/gewijzigd door personen binnen en/of buiten de onderzoeksorganisatie;

3. **Availability (beschikbaarheid)** – Gegevens zijn beschikbaar op die plaatsen waar dat noodzakelijk is voor de bedrijfsvoering van een onderzoeksorganisatie, zoals het ondersteunen van klanten, en/of noodzakelijk voor voorgeschreven beschikbaarheidseisen vanuit wet- en regelgeving.

4. **Accountability (controleerbaarheid)** – De mogelijkheden om met voldoende zekerheid vast te kunnen stellen of wordt voldaan aan de eisen van vertrouwelijkheid, integriteit en beschikbaarheid;

Gegevensbescherming is een organisatiebrede verantwoordelijkheid. Alle gebruikers van de systemen en toepassingen van een onderzoeksorganisatie zijn verplicht mee te werken aan het betrouwbaar houden van deze systemen en toepassingen en een correcte naleving van wet- en regelgeving op het gebied van de bescherming van persoonsgegevens.

De principes voor gegevensbeveiliging worden ondersteund door de zogeheten ‘Plan-do-check-act-cyclus’, die verderop in dit document besproken wordt. Via deze cyclus kunnen onderzoeksorganisaties concreet bepalen welke beveiligingsmaatregelen moeten worden genomen, afhankelijk van de risico’s en de controle van de effectiviteit en naleving daarvan.

ISO normen

ISO is een internationaal systeem bestaande uit normen die worden toegepast voor standaardisering. Indien een bedrijf een bepaald ISO certificaat heeft dan weet een (potentiële) opdrachtgever aan welke standaarden het bedrijf voldoet. Voor marktonderzoek is ISO 20252:2012 een bekende norm die duidelijk maakt welke (persoons)gegevensstromen ontstaan en hoe daarmee moet worden omgegaan. ISO 20252:2012 geeft algemene, niet-gespecificeerde aanbevelingen voor databeveiliging. Op het gebied van databeveiliging zijn de normen ISO 27001 en ISO 27002 veel specifieker.

Is ISO 27001 of ISO 27002 verplicht? Nee, ISO27001/27002 is geen verplichting. Het zijn normen die voor de opdrachtgever duidelijk maken dat de betreffende onderzoeksorganisatie haar databeveiliging goed op orde heeft. Sommige (grote) bedrijven verwachten of eisen dat hun dienstverleners, waaronder onderzoeksorganisaties, aan deze ISO normen voldoen. Het is aan de onderzoeksorganisatie om te beslissen of haar beveiligingsbeleid op het niveau van ISO 27001/27002 gebracht en eventueel gecertificeerd moet worden.

Databeveiliging: een operationele toelichting

Veel ISO onderwerpen op het gebied van databeveiliging zijn ‘high-level’ beschreven. In dit document wordt een meer operationele toelichting gegeven. De volgende onderwerpen komen daarin onder meer ter sprake:

Informatiebeveiligingsbeleid
Er dient een informatiebeveiligingsbeleid te zijn dat gedeeld wordt met partijen waarvoor dit relevant is. Dit beleid moet periodiek worden getoetst op adequaatheid en doeltreffendheid o.a. naar aanleiding van in- en/of externe ontwikkelingen.

Interne organisatie
Het is van belang dat functiescheiding is doorgevoerd. Het dient duidelijk te zijn wie op het gebied van informatiebeveiliging voor wat verantwoordelijk is (bijvoorbeeld juridische aspecten of technische aspecten). De interne organisatie dient zo ingericht te zijn dat informatiebeveiliging bij ieder type project is geborgd.

Mobiele apparatuur
Er dient een beleid te zijn dat aangeeft hoe omgegaan wordt met mobiele apparatuur, en wat de spelregels zijn indien het bedrijf toestaat dat er vanaf een andere locatie gewerkt wordt dan vanuit de bedrijfslocatie zelf (bijvoorbeeld thuiswerken).

Personeel
Het personeel van een onderzoeksorganisatie dient op relevante aspecten gescreend te zijn. Er dient een geheimhoudingsovereenkomst te zijn met elk personeelslid en er dient een sanctiebeleid te zijn geformuleerd in het geval van overtredingen met betrekking tot informatiebeveiliging. De onderzoeksorganisatie moet aantoonbaar kunnen maken hoe en op welke wijze zij werkt aan het verhogen van het informatiebeveiligingsbewustzijn van alle medewerkers.

Beheer van bedrijfsmiddelen
Er dient een overzicht te zijn van bedrijfsmiddelen die informatie bevatten (bijvoorbeeld smartphones) of die gebruikt worden bij informatieverwerking (bijvoorbeeld laptops). Per bedrijfsmiddel moet duidelijk zijn wie ervoor verantwoordelijk is. De regels voor het gebruik van deze middelen dienen transparant te zijn. Er dient een regeling te zijn die zeker stelt dat verstrekte bedrijfsmiddelen worden ingeleverd wanneer een medewerker uit dienst treedt.

Informatieclassificatie
Informatiesoorten moeten met betrekking tot vertrouwelijkheid, integriteit en beschikbaarheid voorzien zijn van een impactscore. Met behulp van deze classificaties kan bewust gekozen worden voor een passend niveau van beveiliging. Het moet duidelijk zijn wat het vertrouwelijkheidskarakter is van een informatiesoort (variërend van geheim tot openbaar).

Behandelen van media
Voor het beheren van verwijderbare media (bijvoorbeeld een usb-stick) moeten procedures aanwezig zijn in overeenstemming met het hiervoor genoemde informatieclassificatieschema. Media moeten op een veilige manier worden verwijderd als deze niet langer benodigd zijn. Media die informatie bevatten, moeten worden beschermd tegen onbevoegde toegang of bewerking tijdens hun transport.

Logische toegangsbeveiliging
Er dient een beleid voor logische toegangsbeveiliging te zijn waarmee zeker wordt gesteld dat gebruikers alleen toegang krijgen tot dat deel van het netwerk waarvoor zij bevoegd zijn. In dit kader dient een formele registratie- en uitschrijvingsprocedure aanwezig te zijn voor het toekennen van autorisaties. De uitgegeven autorisaties moeten periodiek beoordeeld worden en eventueel herzien.

Toegangsbeveiliging van systemen
Er dienen beveiligde inlogprocedures te zijn. Systemen voor wachtwoordbeheer moeten interactief zijn en 'sterke' wachtwoorden waarborgen. Het gebruik van speciale systeemhulpmiddelen die in staat zijn om beheersmaatregelen te omzeilen moet worden beperkt en nauwkeurig worden gecontroleerd. Dit geldt ook voor de toegang tot programmabroncodes.

Fysieke beveiliging
Binnen kantoren en andere ruimten moeten beveiligingszones worden gedefinieerd en passende maatregelen worden genomen om informatie en informatieverwerkende faciliteiten te beschermen. Speciale aandacht is nodig voor mogelijk ongecontroleerde ingangen (zoals laad- en loslocaties), alsmede het ('s avonds) betreden van de bedrijfsruimte door opdrachtgevers en respondenten tijdens kwalitatieve onderzoeksessies en het 's avonds betreden van de bedrijfsruimte door (freelance) telefonische interviewers.

Apparatuur
Apparatuur moet zo worden geplaatst en beschermd dat risico's van bedreigingen van buitenaf of de kans op onbevoegde toegang worden verkleind. Apparatuur en bijbehorende bekabeling moet goed worden onderhouden. Ook is aandacht nodig voor apparatuur die zich buiten de bedrijfsruimte bevindt. Clear desk en clear screen beleid is noodzakelijk en dient bekend te zijn bij de betreffende medewerkers.

Beveiliging van bedrijfsvoering
Waar nodig moeten gedocumenteerde beveiligingsprocedures beschikbaar zijn. Veranderingen in de organisatie, bedrijfsprocessen, informatieverwerkende faciliteiten en systemen moeten worden beheerst. Het gebruik van middelen moet worden gemonitord om de vereiste systeemprestaties te waarborgen. Ontwikkel-, test- en productieomgevingen moeten zijn gescheiden om het risico op onbevoegde toegang te verlagen. Ter bescherming tegen malware moeten beheersmaatregelen voor detectie, preventie en herstel zijn ingevoerd, in combinatie met een passend bewustzijn van gebruikers (social engineering).

Regelmatig moeten backups worden gemaakt en getest. Logbestanden van gebeurtenissen moeten worden gemaakt, bewaard en regelmatig worden beoordeeld. Loginformatie moet passend worden beschermd. Activiteiten van systeembeheerders moeten worden gelogd.

Technische kwetsbaarheden
Informatie over technische kwetsbaarheden moet tijdig worden verzameld en passende maatregelen moeten indien nodig worden genomen. Voor het door gebruikers installeren van software moeten regels zijn vastgesteld. Auditeisen en –activiteiten die verificatie van systemen met zich meebrengen moeten zo worden gepland dat deze de bedrijfsprocessen zo min mogelijk verstoren.

Communicatiebeveiliging
Netwerken moeten worden beheerd om informatie in systemen en toepassingen te beschermen. Er dient een passende scheiding in netwerken aanwezig te zijn. Er dient een helder protocol te zijn over de wijze van informatieuitwisseling en de bijhorende maatregelen (bv. 2-factor authenticatie).
Informatie die gedeeld wordt via een openbaar netwerk moet beschermd zijn tegen frauduleuze activiteiten van derden. Informatie die is opgenomen in elektronische berichten moet passend beschermd zijn.

Beveiligingseisen voor informatiesystemen
Er dient een beleid te zijn voor het veilig ontwikkelen van software en systemen. Principes voor engineering moeten worden vastgesteld. Als bedieningsplatforms zijn veranderd, moeten bedrijfskritische toepassingen worden beoordeeld en getest om te waarborgen dat er geen nadelige impact is. Uitbestede systeemontwikkeling moet onder supervisie van de onderzoeksorganisatie staan en moet gemonitord worden. Tijdens de ontwikkelactiviteiten moet de

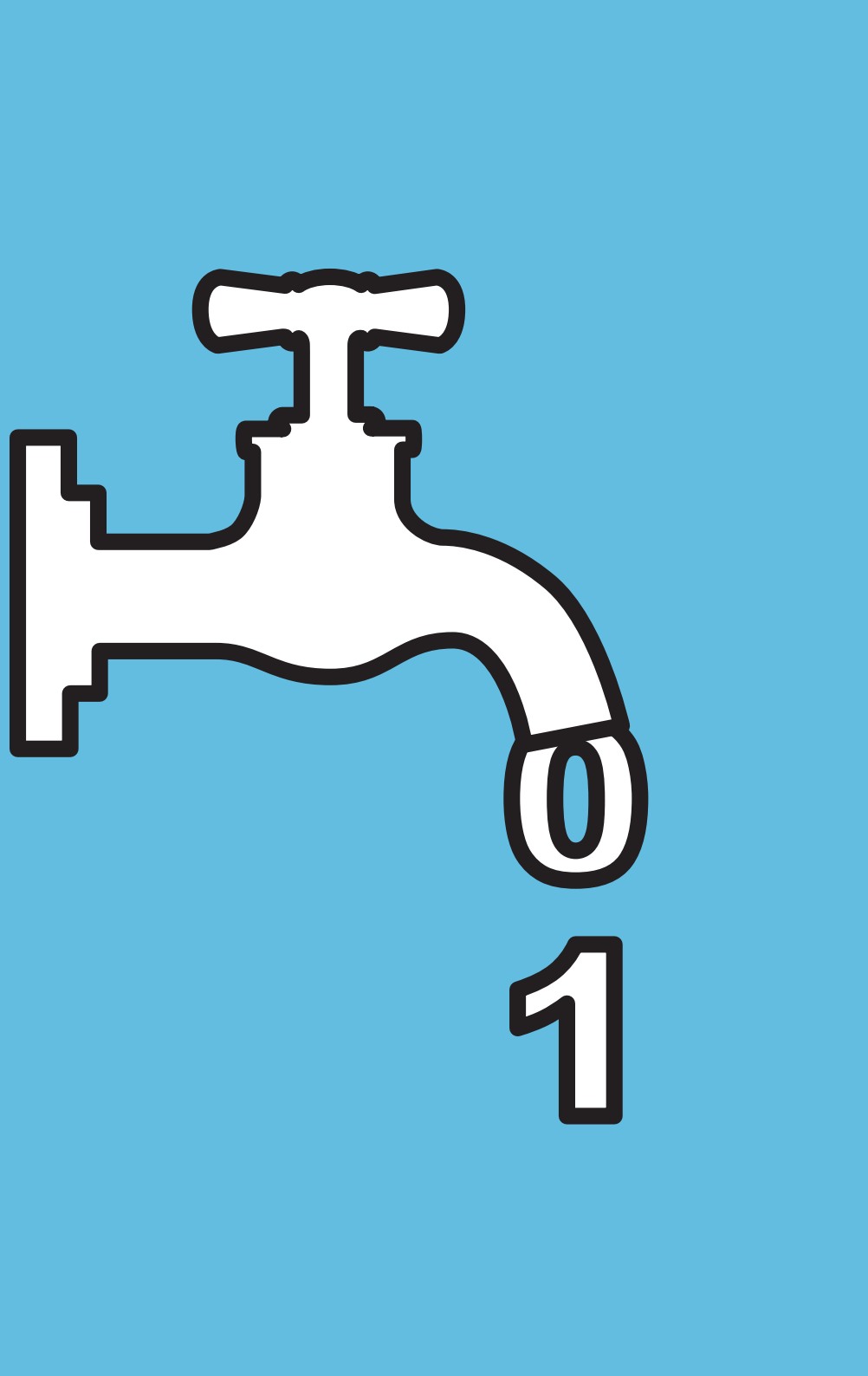
beveiligingsfunctionaliteit worden getest. De gebruikte testgegevens moeten beschermd worden.
Voordat nieuwe informatiesystemen, upgrades en nieuwe versies live gaan, moet een acceptatietest worden uitgevoerd.

Relaties met leveranciers en opdrachtgevers
Met de leveranciers en de opdrachtgevers moeten de informatiebeveiligingseisen worden overeengekomen. De dienstverlening van de leveranciers moet worden gemonitord en regelmatig worden beoordeeld. Veranderingen in de dienstverlening van leveranciers en de dienstverlening aan opdrachtgevers moeten worden beheerd, rekening houdend met het afbreukrisico van informatie, systemen en processen.

Beheer van informatiebeveiligingsincidenten
Er moet een procedure zijn die een snelle en doeltreffende respons op incidenten bewerkstelligt. Informatiebeveiligingsgebeurtenissen moeten worden beoordeeld en er moet worden vastgesteld of deze moeten worden geclassificeerd als informatiebeveiligingsincidenten. Kennis die is verkregen door deze incidenten te analyseren en op te lossen moet worden gebruikt om de waarschijnlijkheid en/of de impact van toekomstige incidenten te verkleinen.

Informatiebeveiligingscontinuïteit
De organisatie moet de eisen voor informatiebeveiliging en continuïteit in geval van een calamiteit vaststellen. Op basis van deze eisen moeten passende maatregelen doorgevoerd worden die regelmatig op hun werking worden getoetst. Informatieverwerkende faciliteiten moeten met voldoende redundantie worden uitgevoerd.

Naleving
Alle relevante wet- en regelgeving moet worden vastgesteld en de wijze van borging daarvan moet transparant zijn. Registraties moeten in overeenstemming met wettelijke eisen en bedrijfseisen en moeten worden beschermd tegen verlies, vernietiging , onbevoegde toegang en onbevoegde vrijgave. Privacy, bescherming van persoonsgegevens en cryptografische beheersmaatregelen moeten worden gewaarborgd in lijn met relevante wet- en regelgeving.



Autoriteit Persoonsgegevens: beleidsregels beveiliging en datalekken

De toezichthouder in Nederland op het gebied van bescherming en beveiliging van persoonsgegevens is de Autoriteit Persoonsgegevens (AP) gevestigd in Den Haag (www.autoriteit persoonsgegevens.nl). De AP heeft beleidsregels gepubliceerd op het gebied van beveiliging (de Beleidsregel Beveiliging en de Beleidsregel Datalekken).

Beleidsregel Beveiliging
De Autoriteit Persoonsgegevens heeft richtsnoeren voor beveiliging van persoonsgegevens gepubliceerd: https://autoriteitpersoonsgegevens.nl/nl/richtsnoeren-beveiliging-van-persoonsgegevens-2013

Deze dienen mede als uitgangspunt voor de beveiliging van persoonsgegevens in de onderzoeksorganisatie. Hiertoe hanteert de onderzoeksorganisatie een 'Plan-do-check-act-cyclus'.

Beleidsregels Meldplicht Datalekken
De Autoriteit Persoonsgegevens heeft beleidsregels omtrent de meldplicht in het geval van datalekken gepubliceerd: https://autoriteitpersoonsgegevens.nl/nl/melden/meldplicht-datalekken#publications

Bij een datalek gaat het om een inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens. Onder een datalek valt dus niet alleen het vrijkomen (lekken) van gegevens, maar ook de onrechtmatige verwerking van gegevens.

Er is sprake van een datalek als er een inbreuk is op de beveiliging van persoonsgegevens (zoals bedoeld in artikel 4 lid 12 AG). Bij een datalek bestaat de mogelijkheid dat persoonsgegevens verloren gaan of onrechtmatig verwerkt worden, dus datgene waartegen de beveiligingsmaatregelen bescherming moeten bieden.

Voorbeelden van datalekken zijn een verloren USB-stick met persoonsgegevens, een gestolen laptop of een inbraak in een databestand door een hacker.

Niet alle datalekken moeten gemeld worden bij de Autoriteit Persoonsgegevens. Een inbreuk op de beveiliging melden bij de Autoriteit Persoonsgegevens en de betrokkene is noodzakelijk tenzij het niet waarschijnlijk is dat de inbreuk in verband met persoonsgegevens een risico inhoudt voor de rechten en vrijheden van natuurlijke personen. Een melding aan de betrokkenen kan eventueel achterwege worden gelaten indien één van de volgende voorwaarden is vervuld;

a) als er passende technische beschermingsmaatregelen zijn getroffen, en deze maatregelen zijn toegepast op de persoonsgegevens waarop de inbreuk betrekking heeft, met name die welke de persoonsgegevens onbegrijpelijk maken voor onbevoegden, zoals versleuteling/encryptie.
b) de verwerkingsverantwoordelijke achteraf maatregelen heeft genomen om ervoor te zorgen dat het bedoelde hoge risico voor de rechten en vrijheden van betrokkene zich waarschijnlijk niet meer zal voordoen.
c) de mededeling een onevenredige inspanning vergt. In dat geval komt er in de plaats daarvan een openbare mededeling of een soortgelijke maatregel waarbij de personen even doeltreffend worden geïnformeerd.

Alle interne en externe gebruikers van randapparatuur, gegevens en systemen, of gebruikers die optreden namens de onderzoeksorganisatie, zijn verplicht (beveiligings-) incidenten en/of potentiële risico's onmiddellijk te melden bij hun direct leidinggevende en/of de daartoe aangewezen functionaris van de onderzoeksorganisatie. Hiervoor dient binnen de onderzoeksorganisatie een aparte procedure te worden opgesteld. In de MOA Verwerkersovereenkomst is een protocol voor melding van datalekken opgenomen.

Verwerkersovereenkomst

Indien derden worden ingeschakeld bij het verwerken van persoonsgegevens, zoals een onderzoeksorganisatie, worden deze derden in het algemeen beschouwd als een verwerker. De verplichtingen met betrekking tot beveiliging dienen door de opdrachtgever/verwerkingsverantwoordelijke voor de gegevensverwerking te worden voorgelegd aan de verwerker middels een Verwerkersovereenkomst. Een voorbeeld van zo'n Verwerkersovereenkomst (de MOA Verwerkersovereenkomst) maakt deel uit van deze MOA Richtlijn Data Beveiliging.

Cloudopslag

Bij het in de cloud opslaan van persoonsgegevens dient de onderzoeksorganisatie daarover transparant te zijn naar haar opdrachtgevers. Wordt de cloud gehost buiten de Europese Unie, en/of in een als onveilig beschouwd land (in termen van digitale infrastructuur), dan dienen aanvullende (contractuele) afspraken te worden gemaakt met de opdrachtgever.

Panels

Een aantal onderzoeksorganisaties beschikt over een eigen panel. Uiteraard gelden de eisen op het gebied van databeveiliging ook voor dat panel. Een Verwerkersovereenkomst is niet nodig, omdat het om een eigen panel van de onderzoeksorganisatie gaat.

Soms hebben opdrachtgevers een eigen panel dat beheerd wordt door een onderzoeksorganisatie, waarbij de taken met betrekking tot het panel verdeeld zijn tussen opdrachtgever/paneleigenaar en de onderzoeksorganisatie. In dit geval is een Verwerkersovereenkomst tussen opdrachtgever en de onderzoeksorganisatie wel noodzakelijk.

Tenslotte zijn er ook 'sample only' panels die hun diensten aan onderzoeksorganisaties aanbieden. In deze gevallen is er geen noodzaak om een Verwerkersovereenkomst op te stellen. Immers, bij een dergelijk panel worden alleen onderzoeksuitkomsten (antwoorden op gestelde vragen) opgeleverd en per definitie geen identificerende persoonsgegevens.

‘Plan-do-check-act-cyclus’
Voor een blijvend passend beveiligingsniveau is het hanteren van de zogeheten plan-do-check-act- cyclus in de dagelijkse praktijk van de organisatie noodzakelijk.

Deze cyclus komt op het volgende neer:

1 Beoordeel de risico’s
Beoordeel de risico’s die de gegevens en de aard van de verwerking met zich meebrengen voor de betrokkenen en bepaal op basis daarvan het gewenste beveiligingsniveau. Inventariseer vervolgens de dreigingen die kunnen leiden tot een beveiligingsincident, de gevolgen die het beveiligingsincident kan hebben en de kans dat deze gevolgen zich voor zullen doen. Tref op basis daarvan gericht beveiligingsmaatregelen die het gewenste beveiligingsniveau kunnen waarborgen.

2 Maak gebruik van algemeen geaccepteerde beveiligingsstandaarden
Het vakgebied informatiebeveiliging kent vele beveiligingsmethoden, -standaarden en -maatregelen die zijn gebaseerd op ervaringen uit de dagelijkse beveiligingspraktijk. Gebruik bij het nemen van beveiligingsmaatregelen de richtsnoeren in samenhang met de beschikbare beveiligingsstandaarden,zoals bijvoorbeeld ISO 27001. Deze standaard geeft houvast bij het daadwerkelijk treffen van passende maatregelen om de beveiligingsrisico’s af te dekken.

3 Controleer en evalueer regelmatig
Controleer met zekere regelmaat of de beveiligingsmaatregelen daadwerkelijk zijn getroffen en worden nageleefd. Beoordeel periodiek of het beveiligingsniveau nog steeds past bij de risico’s die de verwerking en de aard van de te verwerken gegevens met zich meebrengen en of de beveiligingsmaatregelen nog steeds voldoen. Betrek daarbij ook de stand van de techniek en de nieuwste inzichten binnen het vakgebied informatiebeveiliging. Pas waar nodig de beveiligingsmaatregelen aan.

Bijlagen bij MOA
Richtlijn Data Beveiliging

Bijlage 1

Beveiliging en Internet

Gebruikers van internettoepassingen, die aan hen ter beschikking zijn gesteld, dienen zich ervan bewust te zijn dat veel websites technologie gebruiken waarmee het mogelijk wordt om interactieve acties uit te voeren, gebruikersvoorkeuren te bemachtigen of persoonlijke informatie te vergaren. De gebruikte technologieën hiervoor zijn bijvoorbeeld Java applet en ActiveX componenten. Zodra bepaalde functies op een webpagina worden gebruikt, kunnen kleine programma's gedownload worden vanaf de server naar de gebruiker en vandaar op het lokale systeem draaien. Dergelijke programma's kunnen zijn geconfigureerd om gebruikersinformatie te uploaden naar het internet, zonder dat de gebruiker hier weet van heeft. Hiervoor is de cookiebepaling in artikel 11.7a Telecommunicatiewet opgesteld.

Gebruik Internet door medewerkers en freelancers van onderzoeksorganisaties

1. Wanneer het de bedrijfsvoering baat, kan het zijn dat de onderzoeksorganisatie zijn medewerkers op het internet onderwerpen laat uitzoeken die relevant zijn voor bedrijfsfuncties. Ook kunnen zij deelnemen aan forums, nieuwsgroepen en andere informatie-uitwisselingslocaties, die professionele bekwaamheid bevorderen, in belangrijke informatie voorzien en/of voor voortgang in -voor de onderzoeksorganisatie relevante- projecten zorgen, met inachtneming van het bepaalde in dit document.
2. Internetcommunicatie door medewerkers van de onderzoeksorganisatie mag nimmer beschadigende informatie bevatten, evenals intimiderend of andersoortig negatief taalgebruik of zaken waardoor de naam en/of bedrijfsvoering en/of klant- en cont(r)acten van een onderzoeksorganisatie in een negatief daglicht komen te staan. Alle informatie, over het internet gecommuniceerd, mag de bedrijfsvoering van een onderzoeksorganisatie en/of anderen niet verstoren of beschadigen. Dit geldt in het bijzonder ook voor het gebruik van social media.
3. Het wordt zeer sterk afgeraden om informatie te (trachten te) bemachtigen die aanstootgevend is, evenals websites te bezoeken waarvan verwacht kan worden dat aanstootgevende informatie wordt getoond.
4. Wanneer het internet als communicatiemiddel gebruikt wordt om respondenten te bereiken, dient vooraf vastgesteld te worden wat de risico's zijn van het gebruik van dit medium en moet getoetst te worden of wordt voldaan aan toepasselijke wetgeving. Dit wordt gedaan door of samen met de daartoe aangewezen functionaris van de onderzoeksorganisatie.
5. Software patches en upgrades dienen alleen door systeembeheer te worden gedownload, en alleen vanaf sites van leveranciers waarmee de onderzoeksorganisatie onderhoudscontracten heeft gesloten.
6. Alle software copyright wetgeving (zowel Nederlandse als internationaal) dient te worden nagevolgd. Het is niet toegestaan om met copyright beschermde software te distribueren en/of kopiëren tenzij hiervoor expliciet en uitdrukkelijk toestemming is verleend, of de juiste licentie daarvoor is verleend.

Uitwisselen en/of verstrekken van persoonsgegevens (informatie)

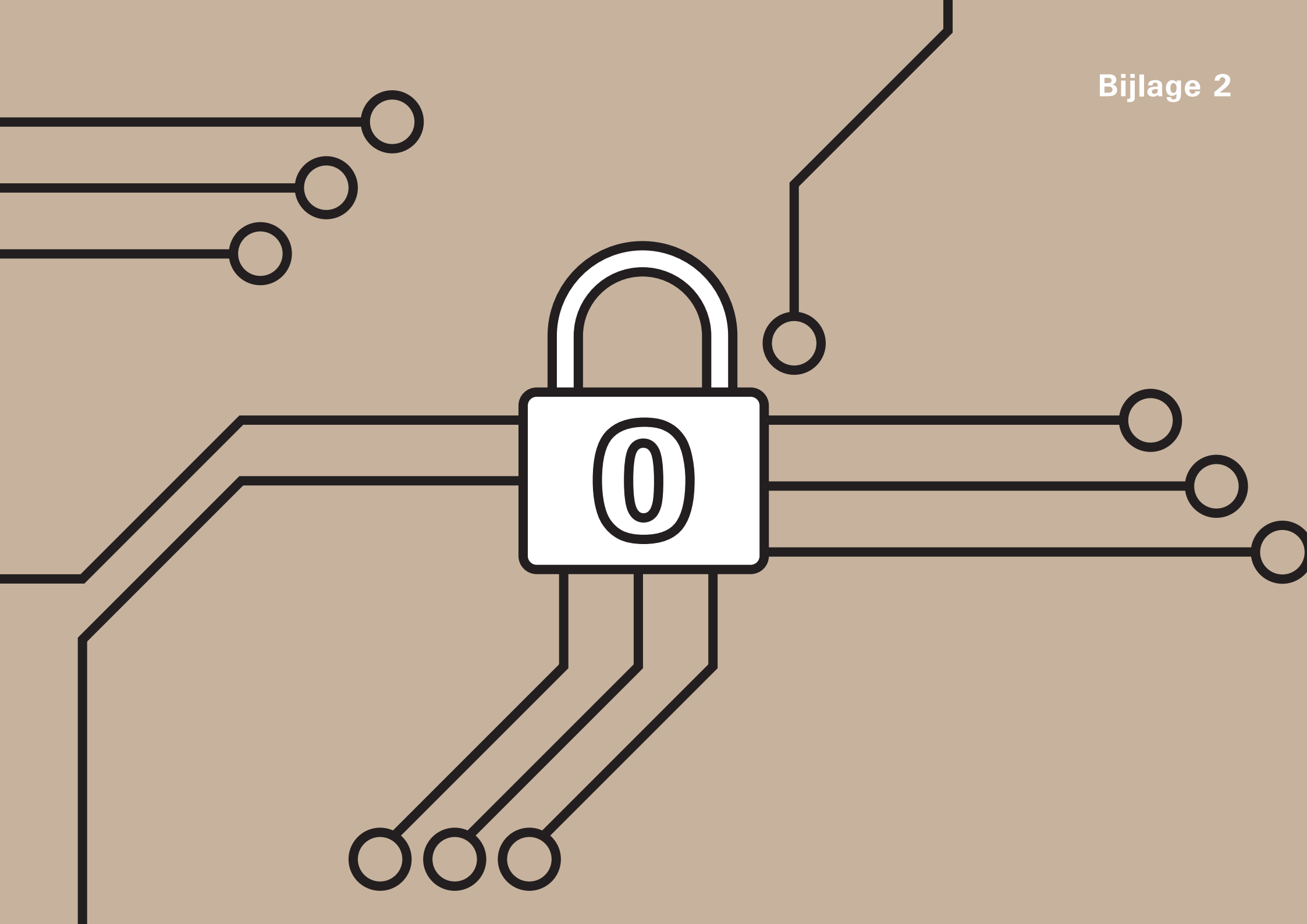
1. Bijzondere, gevoelige en/of vertrouwelijke informatie die identificerend is, behoort niet via het internet verzonden te worden, tenzij er beschikking is over een voldoende beveiligde werkwijze. Hieronder verstaan we publieke/privé versleuteling, key encryption algoritmen of een beveiligde omgeving waar de opdrachtgever zelf deze informatie kan ophalen via een beveiligde verbinding (zgn. secure FTP-server).
2. Overweeg goed voorafgaande aan verzending van gevoelige en/of vertrouwelijke informatie of de beveiliging voldoende is. Wachtwoordvoorzieningen op originele bestanden zelf, zoals Zip bestanden, Word documenten, Excel spreadsheets, enz., zijn, op zichzelf staand, geen (en worden niet beschouwd als) afdoende beveiligingsoplossingen voor verzending via het internet. Dit geldt specifiek in de gevallen waar de informatie een combinatie betreft van persoonsgegevens (identificerend) met andere gevoelige en/of vertrouwelijke persoonsgegevens.

Onacceptabel gebruik van internet binnen de onderzoeksorganisatie

De hierna volgende lijst beschrijft enkele mogelijke acties die als onacceptabel gebruik van de infrastructuur voor een onderzoeksorganisatie worden beschouwd:

1. Het gebruiken van door de onderzoeksorganisatie beschikbaar gestelde middelen en/of internetverbinding voor eigen privéactiviteiten of handelsactiviteiten, zoals het exploiteren van een webshop, het opslaan van (strafbare of auteursrechtelijk beschermde) afbeeldingen of het uploaden van eigen software.
2. Het aanmaken en/of verspreiden van kettingbrieven, junkmails (spam) of soortgelijke correspondentie.
3. Het (trachten te) verkrijgen van ongeautoriseerde toegang tot een of meerdere computersystemen voor een onderzoeksorganisatie of welke andere organisatie dan ook.
4. Het versturen van racistische en/of discriminerende en/of (seksueel) intimiderende en/of bedreigende berichten.
5. Het downloaden, bekijken en/of verspreiden van pornografisch (beeld-) materiaal.

Bijlage 2



Technische en organisatorische maatregelen

Beveiliging is een samenspel van technische en organisatorische maatregelen. In dit deel wordt ingegaan op enkele vaak voorkomende technische en organisatorische maatregelen die worden getroffen om te voldoen aan de principes van beveiliging.

Encryptie en hashing

De onderzoeksorganisatie dient zich maximaal in te spannen om persoonsgegevens te beveiligen die worden verwerkt. Hierbij wordt aanbevolen om bijvoorbeeld bijzondere persoonsgegevens te beveiligen door deze geëncrypteerd op te slaan en geëncrypteerd te verzenden of om gebruik te maken van een SFTP server. Het wordt de onderzoeksorganisatie aanbevolen om encryptie (versleuteling) toe te passen bij verzending van persoonsgegevens via internet, de opslag van gegevens op draagbare apparatuur en op verwijderbare media zoals usb-sticks en in andere situaties waar persoonsgegevens kwetsbaar zijn voor toegang door onbevoegden. Encryptie wordt tevens dringend aanbevolen in gevallen waar het gaat om persoonsgegevens met een hoog risico zoals financiële gegevens, bsn-nummers en creditcardnummers.

Bij de opslag en de verwerking maakt de onderzoeksorganisatie onderzoeksorganisatie gebruik van hashing. Bij het toepassen van cryptografische en hashing technieken zal de onderzoeksorganisatie alle gangbare voorzorgsmaatregelen toepassen, zoals goed geregeld sleutelbeheer en het gebruik van sleutellengten en versleutelingstechnieken die in overeenstemming zijn met de actuele stand van de techniek.

Logging en controle

Alle activiteiten die gebruikers uitvoeren op de systemen van een onderzoeksorganisatie, bijvoorbeeld met bestanden van opdrachtgever, worden door de onderzoeksorganisatie vastgelegd in logbestanden. Dit zelfde geldt voor andere relevante gebeurtenissen, zoals pogingen om ongeautoriseerde toegang te krijgen tot gegevens en verstoringen die kunnen leiden tot verminking of verlies van persoonsgegevens. De logbestanden worden periodiek gecontroleerd op indicaties van onrechtmatige toegang of onrechtmatig gebruik van de gegevens en waar nodig wordt actie ondernomen.

Incidentenbeheer

De onderzoeksorganisatie heeft procedures voor het tijdig en doeltreffend behandelen van informatiebeveiligingsincidenten, zoals datalekken en zwakke plekken in de beveiliging, zodra deze zijn gerapporteerd. De lessen uit de afgehandelde incidenten worden gebruikt om de beveiliging structureel te verbeteren. Als een informatiebeveiligingsincident juridische maatregelen tot gevolg heeft, zal de onderzoeksorganisatie zorgen dat bewijsmateriaal wordt verzameld, bewaard en gepresenteerd overeenkomstig de voorschriften voor bewijs die voor het relevante rechtsgebied zijn vastgelegd. In de Verwerkersovereenkomst die in deze publicatie is opgenomen, is een protocol opgenomen dat dient te worden ingevuld indien er sprake is van een datalek. Dit is niet alleen waardevol voor de opdrachtgever (Verantwoordelijke) die onder omstandigheden de Autoriteit Persoonsgegevens dient te informeren, ook de onderzoeksorganisatie kan hiermee haar beveiligingsbeleid verder aanscherpen.

Gebruik wachtwoord

Het is gebruikers niet toegestaan een of meerdere (onderdelen van) wachtwoord beschermingsmiddelen te verwijderen en/of te omzeilen. Wachtwoorden bieden primair bescherming tegen ongeautoriseerde toegang en stellen de gebruiker in staat zich te identificeren als geautoriseerd gebruiker van dat apparaat en/of systeem. Iedere gebruiker is persoonlijk verantwoordelijk voor alle activiteiten die onder zijn/haar gebruikersaccount worden uitgevoerd. De keuze van een zgn. ‘sterk’ wachtwoord en passende geheimhouding hieromtrent, ofwel het niet meedelen van dit wachtwoord aan wie dan ook, helpt misbruik van een account door anderen te vermijden.

Een wachtwoord voor schermbeveiliging is het wachtwoord dat de gegevens op het systeem beschermt, wanneer de gebruiker tijdelijk afwezig is bij de PC. Gebruikers dienen de schermbeveiligingsinstelling, behorende bij het geleverde OS (zoals Windows versies), te hanteren met gebruik van het wachtwoord voor ontkoppeling. Een computer dient altijd vergrendeld te worden, zodra

een gebruiker zijn PC/Laptop verlaat. Aanvullend dient de schermbeveiligingsinstelling dusdanig te zijn geconfigureerd dat, na ten hoogste 15 minuten inactiviteit op het apparaat, de beveiliging automatisch inschakelt. Een uitzondering hierop is bij het geven van presentaties, waarbij de schermbeveiliging tijdelijk op 30 minuten inactiviteit mag worden ingesteld.

E-mailboxen

Een onderzoeksorganisatie wijst aan medewerkers een mailbox toe om te gebruiken voor bedrijfsmatige, werk gerelateerde acties. Hoewel beperkt incidenteel gebruik ervan voor privédoeleinden is toegestaan, dient iedere gebruiker zich ervan bewust te zijn dat van de informatie en berichten die zijn opgeslagen op het systeem, onder omstandigheden, kennis kan worden genomen door functionarissen van een onderzoeksorganisatie. Let op dat de mailboxen van geheimhouders, bijvoorbeeld bedrijfsarts en leden van de OR nimmer worden uitgelezen door anderen.
'Eigendom' van de onderzoeksorganisatie zijn:

- alle (digitale) documenten in de mailbox en in daaraan gekoppelde elektronische mappen, die voor bedrijfsdoeleinden voor de onderzoeksorganisatie of haar opdrachtgevers benodigd kunnen zijn.
- alle documenten met enige bewijsfunctie die in een gerechtelijke procedure een rol kunnen spelen of een feitelijke weergave zijn van feiten.

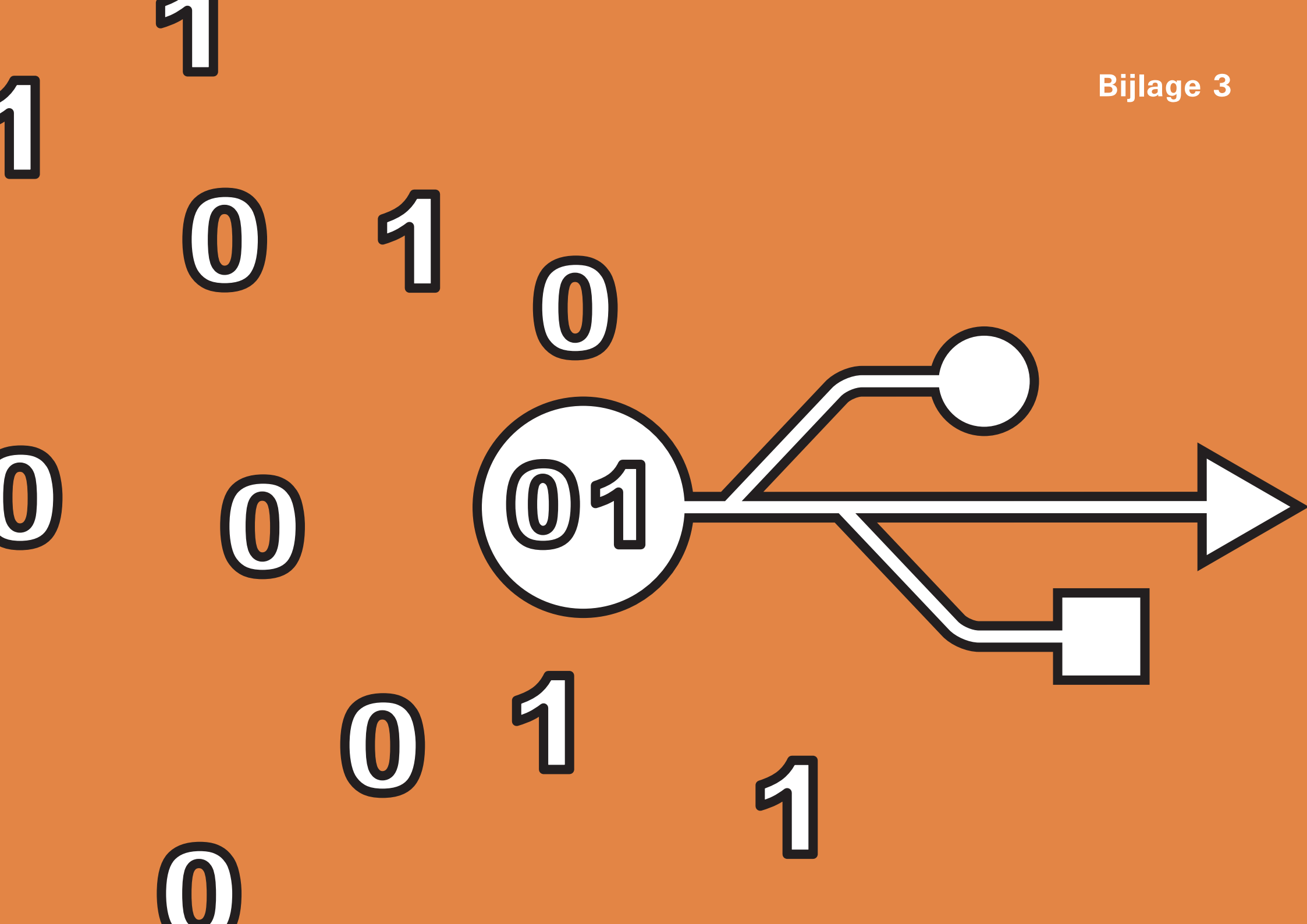
Het is niet mogelijk om vooraf een limitatieve opsomming te geven van (digitale) documenten die hieronder vallen.

Hoewel het onwaarschijnlijk wordt geacht dat er omstandigheden tegelijk optreden, die leiden tot de noodzaak dat de organisatie toegang tot de mailbox van een gebruiker nodig heeft, is het dus wel van belang dat medewerkers/ingehuurde externe medewerkers van een onderzoeksorganisatie zich realiseren dat er geen absolute verwachting van de bescherming van informatie en berichten kan bestaan met betrekking tot de berichten in de mailboxen van deze gebruikers.

Diefstal van data of (rand)apparatuur

Mocht (b)lijken dat randapparatuur gestolen is, ongeacht of dit op kantoor, in een voertuig, privévertrek of elders is voorgevallen, is de werknemer verplicht dit aan de politie te melden en er aangifte van te (laten) doen. Ook dienen de leidinggevenden zo snel mogelijk, doch uiterlijk binnen drie uur, geïnformeerd te worden omtrent het voorval. Een kopie van de aangifte moet aan de leidinggevenden worden overhandigd. Hiervoor is een apart protocol beschikbaar: 'Meldprocedure Datalek' (zie de Verwerkersovereenkomst in dit document).

Bijlage 3



Randapparatuur

Deze bijlage is van toepassing op alle randapparatuur van een onderzoeksorganisatie waarmee toegang wordt verkregen tot de platformen van de onderzoeksorganisatie. Deze bijlage heeft de intentie te voorzien in de minimale standaarden voor de beveiliging van randapparatuur, zoals maar niet beperkt tot PC's, opslagmedia (zoals tapes, tablets en verwijderbare harde schijven) en de software en gegevens die deze apparaten dragen.

De onderzoeksorganisatie stelt randapparatuur ter beschikking voor bedrijfsdoeleinden. Op deze randapparatuur zijn courante, bijgewerkte 'License Agreement' software (bv. Microsoft Windows versie, Word, Excel, PowerPoint en MS Outlook) en andere toepassingen geïnstalleerd. Wanneer aanvullende software benodigd is dient dit middels een verzoek aan de betreffende functionaris kenbaar gemaakt te worden. De aanvraag dient door de leidinggevende van de aanvrager te zijn gefiatteerd. Randapparatuur is/wordt toegewezen aan een gebruiker die vervolgens optreedt als de beheerder van die randapparatuur.

Andere gebruikers kunnen, met toestemming van de betreffende functionaris, onder autorisatie gebruik maken van de betreffende randapparatuur. Binnen de onderzoeksorganisatie wordt gebruik gemaakt van zogenoemde "roaming profiles". Dat betekent dat iedereen die gebruik maakt van een randapparaat zijn eigen profiel gebruikt. Randapparaten kunnen daarmee veilig door meerdere gebruikers worden gedeeld. Gebruikers zijn verantwoordelijk dat geen bestanden buiten de beveiligde omgeving (netwerk, 'my documents' en bureaublad) worden opgeslagen.

Gedeelde verantwoordelijkheden onderzoeksorganisaties en gebruikers

Eindgebruikers dienen erop toe te zien dat:

1. De fysieke beveiliging tot de randapparatuur van de onderzoeksorganisatie in orde is;
2. De gegevens op de randapparatuur beschermd zijn door een correct gebruik van wachtwoord-gebruikersnaam combinatie(s);
3. De antivirus richtlijnen worden opgevolgd;
4. Randapparatuur die frequent gebruikt wordt op de onderzoeksorganisatie netwerkomgeving (niet alleen via VPN), regelmatig de benodigde updates ontvangen en installeren;
5. De politie en de directie van de onderzoeksorganisatie geïnformeerd worden wanneer randapparatuur gestolen (b)lijkt te zijn;

Verantwoordelijkheden van systeembeheerders

Systeembeheerders hebben aanvullende verantwoordelijkheden voor de randapparatuur van de onderzoeksorganisatie, in het bijzonder:

1. Zeker stellen dat alleen geautoriseerde gebruikers toegang hebben tot de juiste "roaming profiles" en dat de gebruikers zich bewust zijn van de bijbehorende verantwoordelijkheden;
2. Zeker te stellen dat antivirus software correct toegepast wordt en werkt;
3. Er op toe te zien dat start- en schermbeveiligingswachtwoorden regelmatig conform beschreven beleid veranderd worden.

Afwijking van deze standaarden kan resulteren in disciplinaire maatregelen, inclusief mogelijke beëindiging van de arbeidsovereenkomst, en mogelijk aanvullende juridische maatregelen.

Notebooks, tablets, smartphone en andere portable randapparatuur

Computerapparatuur, in het bijzonder draagbare computers, laptops of andere randapparatuur waarop gegevens zijn opgeslagen, kunnen bijzonder eenvoudig in handen vallen van anderen door diefstal. Dit brengt potentieel grote financiële gevolgen met zich mee, maar ook het risico is groot dat vertrouwelijke en gevoelige informatie op de betreffende apparatuur in verkeerde handen valt. Hoewel het onmogelijk is om complete bescherming tegen diefstal te implementeren, is het van groot belang dat alle praktisch onderneembare stappen worden gezet om te komen tot een beveiligde omgeving en dat gebruikers gepaste verantwoordelijkheid bij het gebruik van deze apparatuur in acht nemen.

Alle gebruikers zijn verantwoordelijk voor de fysieke conditie van de aan hen toegewezen randapparatuur, en de fysieke bescherming van hun PC en opslagmedia en andere randapparatuur in hun bezit. Wanneer er zeer vertrouwelijke informatie op het apparaat staat, dienen er aanvullende maatregelen genomen te worden voor de fysieke veiligheid. Een gebruiker mag zijn apparatuur niet onbeheerd achterlaten wanneer hij bijvoorbeeld onderweg is. Aan het einde van een werkdag of gedurende langere perioden van afwezigheid dienen alle draagbare apparaten veilig opgeborgen te zijn, met tenminste het gebruik van een (fysiek) slot.

De onderzoeksorganisatie draagt er zorg voor dat alle portable randapparatuur voorzien wordt van een track- en trace functie inclusief een remote wipe functionaliteit. Met een remote wipe functionaliteit, is het mogelijk om data die opgeslagen is op portable randapparatuur in geval van verlies of diefstal te wissen. Met de remote wipe kan portable randaparatuur van afstand gewist worden, om te voorkomen dat de gegevens die zijn opgeslagen op de portable randapparatuur voor onbevoegden beschikbaar komen.

Bring Your Own Device (BYOD)

De onderzoeksorganisatie dient in het kader van toegelaten Bring Your Own Device (aanvullende) effectieve beveiligingsmaatregelen te treffen zowel aan het computersysteem als de BYOD randapparatuur die medewerkers gebruiken.

Voor bijzondere persoonsgegevens en gegevens die als gevoelig worden ervaren, wordt het toelaten van BYOD, afgeraden.

Opslagmedia: externe harde schijf en USB stick

Alle opslagmedia dienen tenminste bewaard te worden conform de hiertoe geldende procedures inzake de bescherming van draagbare PC en randapparatuur beveiliging. Daar deze opslagmedia (doorgaans) niet beschikken over directe beveiligingsmethoden zoals een remote wipe dienen dergelijk opslagmedia opgeslagen te worden achter slot en grendel en zeker niet publiekelijk achtergelaten te worden op een bureau.

Bijlage 4

Aandachtspunten voor systeembeheer

Een goed functionerend beveiligingsbeleid staat of valt met voldoende aandacht voor systeembeheer. Licentiebeheer, back-up en virusbescherming mogen niet aan de individuele gebruiker ter vrije keuze worden overgelaten. Systeembeheer speelt hier een bepalende rol in. Indien een onderzoeksorganisatie te klein is voor een eigen medewerker systeembeheer is het advies om zich aan te sluiten bij een externe organisatie die systeembeheer kan uitvoeren.

Software Licenties

Alle gebruik van de op de onderzoeksorganisatie geïnstalleerde software op randapparatuur dient onder een geldige licentie gedekt te zijn. Zogeheten Site Software License Agreements dekken (het gebruik van) de voorgeïnstalleerde software.

Softwarelicenties worden door Systeembeheer beheerd. De medewerker die in een later stadium eventuele aanvullende software installeert, is ervoor verantwoordelijk dat een geldige licentie beschikbaar is. Het laden en/of installeren van software zonder licentie betekent een inbreuk op auteursrechten en is een overtreding van wet- en regelgeving.

Een ieder die ongeautoriseerd en/of ongelicenseerd software laadt, installeert en/of gebruikt, zal de onderzoeksorganisatie vrijwaren van iedere vorm van claim, aansprakelijkheid, verlies, schade en kosten of uitgaven gerelateerd aan, of als gevolg van, ongeautoriseerd gebruik of kopiëren van software, uitgezonderd van die software die door de onderzoeksorganisatie wordt geleverd.

Back-up: beschikbaarheid van gegevens

Gegevens, die zijn opgeslagen op randapparatuur, kunnen op veel manieren kwijtraken en/of verloren raken. Het is bijvoorbeeld mogelijk dat randapparatuur fysiek verloren gaat of gestolen wordt. Het apparaat kan stukgaan, gegevens kunnen per ongeluk gewist worden of gegevens kunnen door een virus geïnfecteerd en onbruikbaar worden.
Wanneer er geen kopie van de gegevens beschikbaar of opgeslagen is, kan het vele werkuren kosten om dezelfde gegevens weer te (her)creëren, hetgeen kan leiden tot overschrijding van gestelde deadlines etc. Het is de verantwoordelijkheid van alle gebruikers om zeker te stellen dat de gegevens op hun PC accuraat zijn en hersteld kunnen worden ingeval er schade of andersoortig dataverlies optreedt.

Gebruikers hoeven geen back-up te maken van gegevens die zijn opgeslagen op een server van de onderzoeksorganisatie netwerk, of op PC systeembestanden. Deze bestanden worden door Systeembeheer met regelmaat gekopieerd en opgeslagen op ‘master’ schijven. Back-ups van harde schijven dienen tenminste iedere week te worden uitgevoerd. Wanneer gegevens op diskette of DVD/CD-ROM opgeslagen worden dient hiervan op aparte opslagmedia eveneens een back-up te bestaan.

Back-ups dienen te worden opgeslagen op fysiek van de ‘live’ gegevens afgescheiden locaties. Back-ups kunnen bijvoorbeeld bewaard worden op een basislocatie (zoals het kantoor van de gebruiker) terwijl de ‘live’ gegevens bij de gebruiker buiten dat kantoor aanwezig zijn. Back-ups dienen nimmer meegenomen te worden in reguliere notebooktassen of iets dergelijks.

Virus bescherming

Virus detectie software is op iedere PC, en bij voorkeur randapparatuur, geïnstalleerd en continu actief om de gebruikte bestanden te scannen op de aanwezigheid van schadelijk materiaal.
Gebruikers dienen zich er van bewust te zijn dat virus detectie software slechts ongeveer 90% van de bestaande computervirussen direct herkent. Reactieve detectiemaatregelen door alleen antivirus producten zijn duidelijk niet voldoende om het risico op virusinfectie genoeg te migreren. Om schade door virussen te beperken dient iedere gebruiker te handelen conform de onderstaande instructies die betrekking hebben op antivirus en internetgebruik.

Voorkomen van virusinfectie

Alle gebruikers van randapparatuur dienen de virusprogrammatuur op hun systeem actief functionerend te houden.

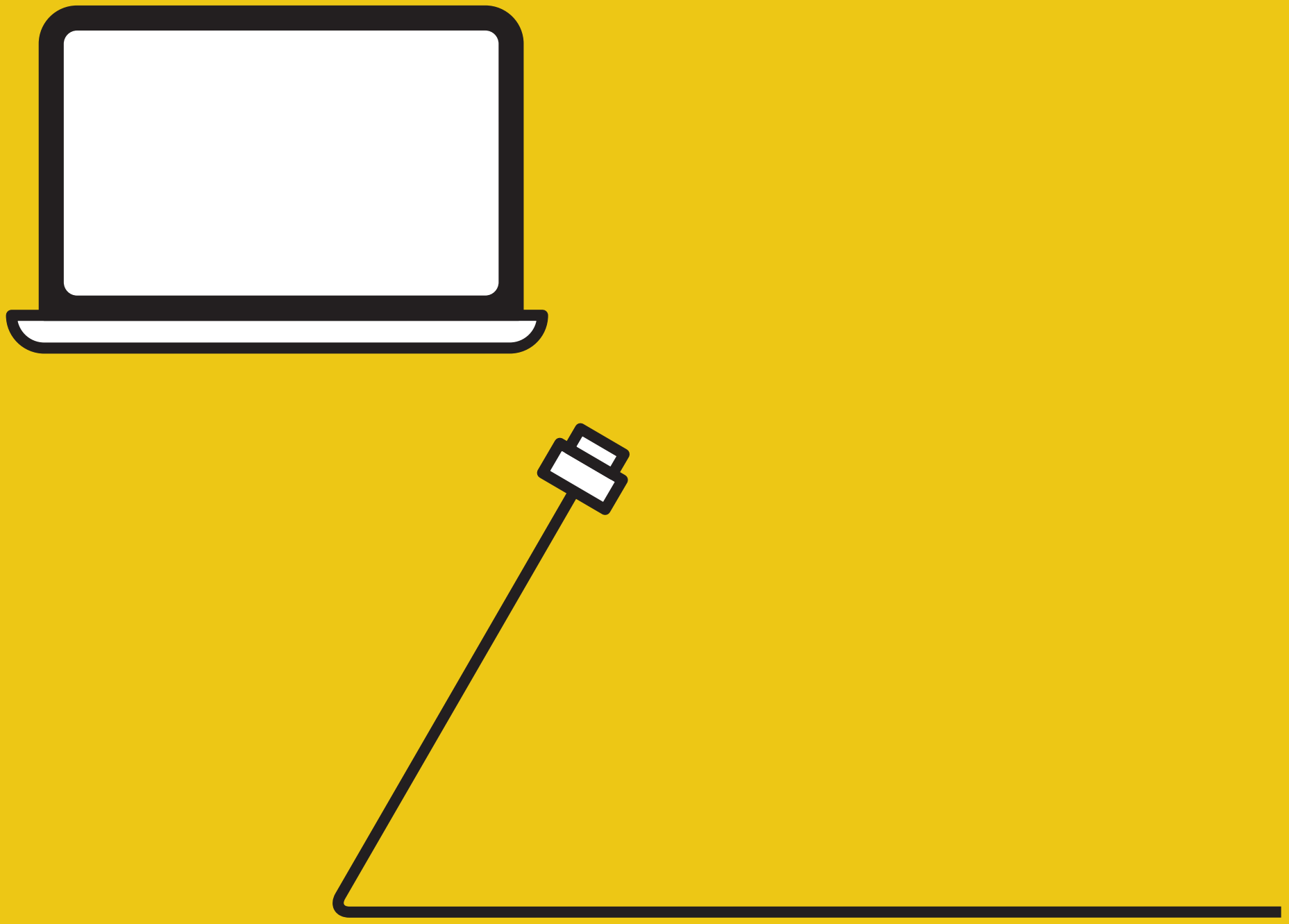
Aanvullend gelden de volgende eisen en adviezen:

1. Gebruikers dienen zich te allen tijde te conformeren aan de richtlijnen voor internetgebruik.
2. Open alleen bijlagen uit een e-mail die afkomstig is van een betrouwbare bron.
3. Wanneer het noodzakelijk is dat een bestandsbijlage gebruikt wordt, dient dit bestand eerst op schijf te worden opgeslagen alvorens actief te gebruiken. Bestandsbijlagen dienen nimmer direct vanuit het bericht geopend te worden. Het eerst opslaan van bestandsbijlagen zorgt ervoor dat de virus detectieprogrammatuur op het system het document of programma scant alvorens het geopend wordt.
4. Gebruikers dienen zich ervan bewust te zijn dat er ook virussen kunnen schuilen in Microsoft Excel en Word macro's, en dergelijke bestanden met een soortgelijke aandacht te behandelen.
5. Software, inclusief shareware/freeware mag alleen door systeembeheerders worden geïnstalleerd.
6. Gaming software, al is het afkomstig van een bekende leverancier, is een algemeen bekende, mogelijke virusdrager en niet toegestaan.
7. Vermijd het direct downloaden van software vanaf het internet.

Hoe te handelen bij een virusaanval?

Wanneer het systeem en/of de gebruiker van een PC/laptop of andere randapparatuur een computervirus heeft gedetecteerd, dient dit onmiddellijk te worden doorgegeven aan de systeembeheerder om verdere verspreiding ervan te voorkomen.

Bijlage 5



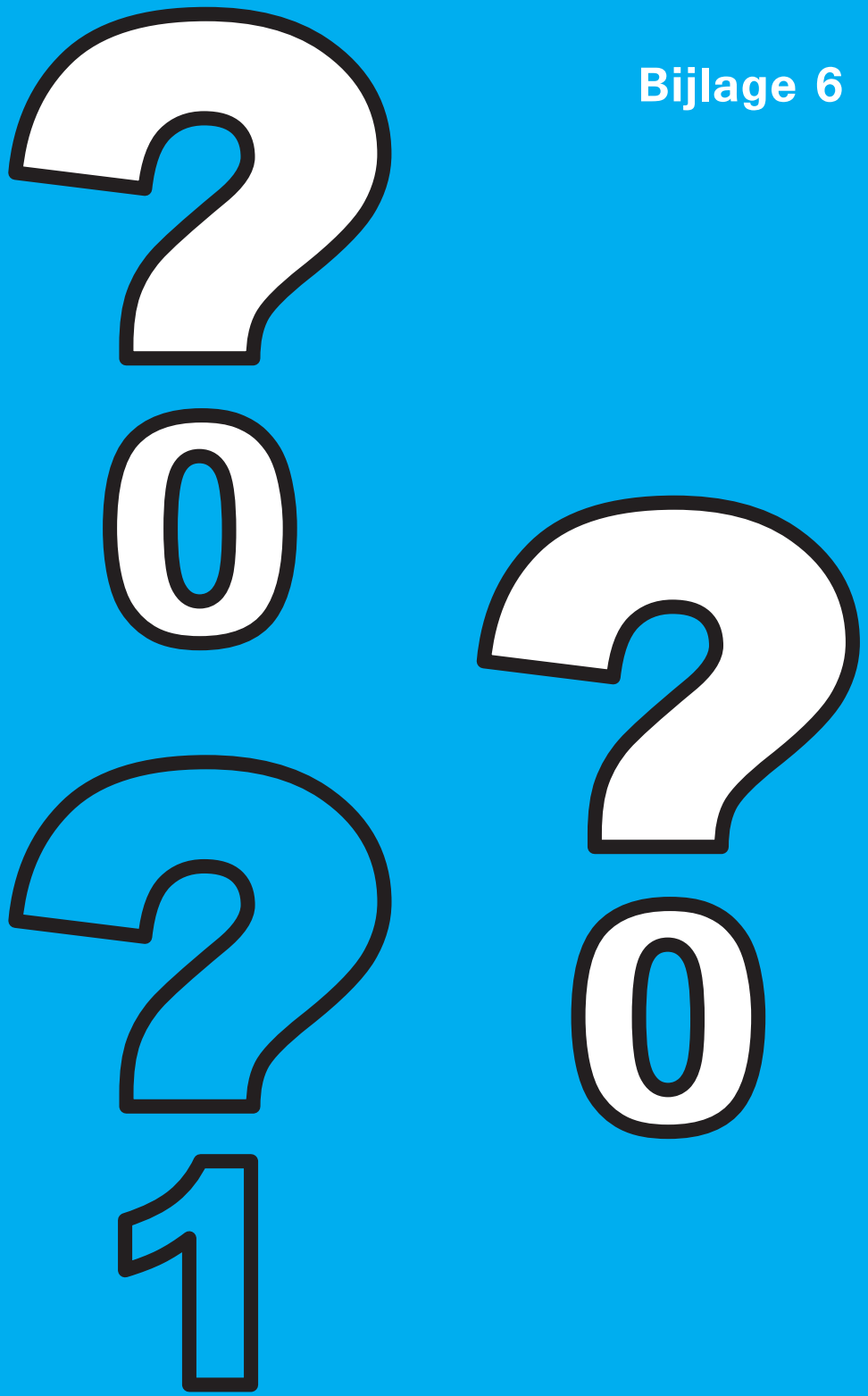
Einde dienstverband

Een belangrijk moment is het einde van een dienstverband of het einde van een opdracht van een externe medewerker. Toegang tot gegevens dient te worden afgesloten, beschikbaar gestelde randapparatuur dient te worden ingeleverd, BYOD randapparatuur zal dienen te worden gewist en (kopieën van) data mogen niet worden achtergehouden door de voormalige medewerker of freelancer.
Bij het beëindigen van een dienstbetrekking of opdracht, ongeacht de reden of aanleiding (uitstroom personeel, ontslag etc.), dient de hiervoor ingerichte procesgang gevolgd te worden. Minimale stappen hierin zijn:

- Backup/overdracht van alle relevante informatie aan een collega en/of opvolger en/of direct leidinggevende.
- Opschoning van alle gegevens.
- Afsluiten externe toegang van medewerker/freelancer.
- Afsluiten e-mailbox, eventueel plaatsen van out-of-office reply met verwijzing naar collega.
- Verzoek aan de vertrekkende medewerker/freelancer om de mailbox bij de werkgever te schonen op privé-berichten.
- Inleveren van alle uitrusting en randapparatuur die door de onderzoeksorganisatie beschikbaar is gesteld.

Systeembeheer draagt er zorg voor dat alle hardware opgeschoond is alvorens deze opnieuw wordt uitgegeven. Alle apparatuur die opslagmedia bevat, zoals laptops of smartphones, wordt ontdaan van de nog eventueel aanwezige gegevens alvorens het apparaat te verwijderen of te hergebruiken. Opslag media met gevoelige persoonsgegevens worden fysiek vernietigd of de persoonsgegevens worden vernietigd, verwijderd of overschreven met technieken die het onmogelijk maken om de oorspronkelijke informatie terug te halen. Dit geldt eveneens voor verwijderbare media, zoals USB-sticks.

Bijlage 6



Veel gestelde vragen en antwoorden

Staat er in de Verwerkersovereenkomst een paragraaf, waar op te letten, do's en don'ts, de valkuilen dus?
Ja, er zijn alternatieven opgenomen voor teksten in de Verwerkersovereenkomst bij de artikelen 3, 5 en 6.

Er staat niets over verzekeringen in het document. Wat moet je dekken en wat wordt er uitgesloten? Ook als verwerker kan je door de verwerkingsverantwoordelijke aansprakelijk worden gesteld. Hoe daar mee om te gaan?
Nee, in de Verwerkersovereenkomst is niets opgenomen over verzekeringen. In artikel 3 van de Verwerkersovereenkomst is de aansprakelijkheid geregeld en worden alternatieven gegeven. U kunt via de MOA wel nadere informatie ontvangen.

Hoe ga je als verwerker om met onderaannemers en subverwerkers?
In de introductie van de Verwerkersovereenkomst wordt deze situatie beschreven. In de Verwerkersovereenkomst is een tekst opgenomen hoe de Verwerkersovereenkomst dient te worden gebruikt bij subverwerkers?

Wie moet het initiatief nemen bij een Verwerkersovereenkomst, wat is handig? Zelf komen met een overeenkomst of dat laten afhangen van de opdrachtgever?
Wettelijk moet de verwerkingsverantwoordelijke voor de gegevensverwerking een Verwerkersovereenkomst voorleggen aan de verwerker. Maar vele verwerkingsverantwoordelijken hebben geen Verwerkersovereenkomst. Het advies is dat verwerker (de onderzoeksorganisatie) de in dit document opgenomen MOA Verwerkersovereenkomst als onderdeel van het contract zal overleggen. Houd rekening met het in deze overeenkomst opgenomen protocol inzake datalekken en leg dat ook voor aan de opdrachtgever.

Kun je volstaan met één contract voor meer opdrachten, dus een soort van mantelovereenkomst of moet je elke keer een nieuwe overeenkomst tekenen?
Zolang de Verwerkersovereenkomst de activiteiten van de verwerker (de onderzoeksorganisatie) maar afdekt, want daar is de verwerker aansprakelijk voor. Doet de verwerker met persoonsgegevens activiteiten die niet zijn opgedragen dan is dat in strijd met de Verwerkersovereenkomst (een toerekenbare tekortkoming) en daarvoor is de verwerker aansprakelijk. Let op indien de verwerker activiteiten doet die niet zijn opgedragen, kan dit ertoe leiden dat de onderzoeksorganisatie zelf verwerkingsverantwoordelijke wordt en alle verplichtingen uit de Algemene Verordening Gegevensbescherming dient na te komen. In de praktijk wordt voor ieder nieuw project een nieuwe Verwerkersovereenkomst opgesteld, bij vervolgprojecten wordt de Verwerkersovereenkomst doorgaans verlengd, en bijlage 1 bij Verwerkersovereenkomst vernieuwd.

Maakt het uit waar het datacenter staat?
Ja, binnen of buiten EU is heel relevant: in de Verwerkersovereenkomst is een bepaling opgenomen over het inschakelen van derden (outsourcing) binnen de EU en buiten de EU. Zowel binnen als buiten de EU is toestemming van de verwerkingsverantwoordelijke nodig die eventueel nadere eisen kan stellen, zoals de toepassing van bijvoorbeeld de EU standard model clauses. Zie artikel 5 en 6 van de in dit document opgenomen Verwerkersovereenkomst.

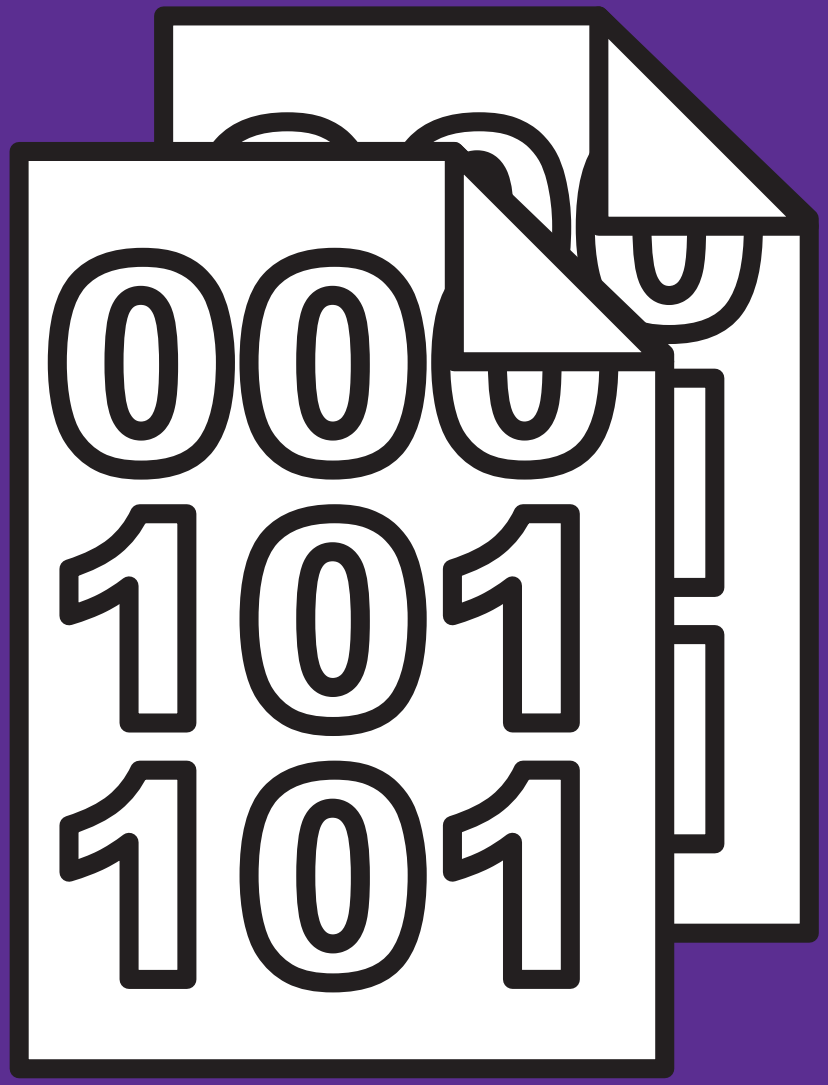
Is er iets over ongeoorloofd gebruik gezegd, wat mag wel en wat niet?
Daar kan men niet in algemene zin iets over zeggen want dat is afhankelijk van het soort gegevens ('bijzondere gegevens' of niet), verenigbaar gebruik, de wijze van rapporteren, etc. Staat het niet beschreven in de Verwerkersovereenkomst, dan is sprake van een toerekenbare tekortkoming van de verwerker en is de verwerker daarvoor aansprakelijk. Bovendien kan de verwerker dan aangemerkt worden als verwerkingsverantwoordelijke en dient dan alle verplichtingen uit de Algemene Verordening Gegevensbescherming na te komen.

Is er een standaard bewaartermijn?
Het is de verwerkingsverantwoordelijke/opdrachtgever die de bewaartermijn zal bepalen. In artikel 1 lid 5 en lid 6 van de Verwerkersovereenkomst zijn concrete termijnen opgenomen inzake het bewaren door de verwerker. Dit zijn veel voorkomende termijnen, indicatief dus. Het doel waarvoor de gegevens worden verwerkt kan soms een langere bewaartermijn rechtvaardigen. Bijlage 1 geeft de verwerkingsverantwoordelijke de mogelijkheid om afwijkende termijnen af te spreken.

Wie mag wat met persoonsgegevens?
In bijlage 1 van de Verwerkersovereenkomst staat omschreven voor welke diensten de verwerker de persoonsgegevens mag gebruiken. Andere diensten/handelingen zijn niet toegestaan. Wat de verwerkingsverantwoordelijke verder doet met de gegevens, daar heeft de verwerker geen zicht op. De Verwerkingsverantwoordelijke bepaalt de doelen en middelen waarvoor hij de persoonsgegevens verwerkt.

Hoe verhouden leveringsvoorwaarden zich tot de Verwerkersovereenkomst?
Voor de Verwerkersovereenkomst wordt de toepasselijkheid van algemene inkoop- of verkoopvoorwaarden uitgesloten. De bepalingen in de Verwerkersovereenkomst prevaleren boven elders vastgelegde afspraken bijvoorbeeld in de opdrachtbevestiging (zie artikel 9 van de in dit document opgenomen Verwerkersovereenkomst).

Hoe om te gaan met de verwerkingsverantwoordelijke die de verwerker wil auditen op beveiliging? Voor wie zijn de kosten?
Hier zijn geen wettelijke regels voor. De kosten komen regulier voor rekening van de verwerkingsverantwoordelijke, tenzij er ernstige tekortkomingen bij de verwerker worden geconstateerd. Dan komen de kosten voor rekening van de verwerker. Deze bepaling is opgenomen in artikel 4 lid 7 van de verwerkersovereenkomst.



Voorbeeld MOA Verwerkersovereenkomst

Concept tekst voor een verwerkersovereenkomst tussen een Verwerkingsverantwoordelijke voor de gegevensverwerking (aangeduid als Opdrachtgever) en een Onderzoeksorganisatie (aangeduid als Verwerker) die namens de verwerkingsverantwoordelijke persoonsgegevens verwerkt, die tot de zeggenschap behoren van de Opdrachtgever.

Opmerking:

Onderstaande verwerkersovereenkomst is een algemene verwerkersovereenkomst die nog aan de specifieke situatie dient te worden aangepast/aangevuld. De onderstaande tekst is een leidraad om te komen tot een verwerkersovereenkomst. Het alleen invullen van de gegevens van de opdrachtgever en de verwerker (onderzoeksorganisatie) is niet voldoende.

Versie 2018: 01, 260118

Verwerkersovereenkomst

De ondergetekenden:

.....,

kantoorhoudende te (.....) .....

aan de .....,

ten deze rechtsgeldig vertegenwoordigd door .....,

hierna te noemen: **“Opdrachtgever”**;

en

.....,

kantoorhoudende te (.....) .....

aan de .....,

ten deze rechtsgeldig vertegenwoordigd door .....,
hierna te noemen: **“Verwerker”**;

Tezamen aangeduid als Partijen

Partijen nemen het volgende in aanmerking:

- Opdrachtgever is als Verwerkingsverantwoordelijke voor de persoonsgegevens op grond van de Algemene Verordening Gegevensbescherming (hierna te noemen: AVG) verplicht een verwerkersovereenkomst aan te gaan met Verwerker.
- In het kader van de tussen partijen afgesproken werkzaamheden vastgelegd in een hoofdovereenkomst, waarvoor deze overeenkomst de schriftelijke verwerkersovereenkomst is, zal Verwerker persoonsgegevens verwerken ten behoeve en in opdracht van de Opdrachtgever zonder aan het rechtstreeks gezag van de Opdrachtgever te zijn onderworpen.
- Verwerker zal bij de uitvoering van de werkzaamheden volgens de instructie en onder verantwoordelijkheid van Opdrachtgever persoonsgegevens verwerken;
- ..... *Andere overwegingen, verwerker is gespecialiseerd in de uitvoering van deze werkzaamheden*
- Opdrachtgever en Verwerker hebben kennisgenomen van de Richtsnoer beveiliging van persoonsgegevens, februari 2013, zie http://wetten.overheid.nl/BWBR0033572/ en artikel 32 AVG om een passend beschermingsniveau te kiezen;
- Aanvullend kunnen schriftelijk andere verwerkingen door Opdrachtgever aan Verwerker worden opgedragen, welke als bijlage aan deze verwerkersovereenkomst zullen worden aangehecht;
- Verwerker zal slechts die gegevensverwerking uitvoeren welke schriftelijk is opgedragen door Opdrachtgever;
- Indien nodig kunnen Opdrachtgever en Verwerker in een aparte overeenkomst of overeenkomsten de overige voorwaarden voor het verrichten van diensten vastleggen;
- Indien in opdracht van de Opdrachtgever meer en andere persoonsgegevens worden verwerkt of indien anders wordt verwerkt dan in bijlage 1 omschreven, geldt deze verwerkersovereenkomst ook voor die verwerkingen en persoonsgegevens.

En komen als volgt overeen:

Artikel 1: Opdracht

1. Opdrachtgever verstrekt opdracht aan Verwerker, welke door verwerker wordt aanvaard om persoonsgegevens te verwerken in overeenstemming met deze overeenkomst.
2. Opdrachtgever blijft de verwerkingsverantwoordelijke voor de gegevensverwerking. Verwerker heeft geen zelfstandige zeggenschap over de gegevens welke voor Opdrachtgever conform deze verwerkersovereenkomst worden verwerkt.
3. Verwerker zal de in Bijlage I genoemde en door Opdrachtgever strikt noodzakelijk verstrekte persoonsgegevens uitsluitend verwerken voor de aldaar omschreven opgedragen werkzaamheden. Indien van toepassing kunnen in deze bijlage tevens aanvullende beveiligingsmaatregelen worden opgenomen die Verwerker zal naleven. BIJLAGE 1 TOEVOEGEN
4. Nadat de opgedragen taken zijn uitgevoerd, zal Verwerker op eerste, schriftelijke verzoek van Opdrachtgever bestanden van verzamelde (persoons)gegevens retourneren en de gemaakte kopieën van persoonsgegevens van Opdrachtgever onmiddellijk vernietigen, tenzij de Opdrachtgever de geleverde dienstverlening en of (persoons)gegevens betwist. Kopieën van persoonsgegevens die onderdeel zijn van de back-up routine van Verwerker dienen zo snel mogelijk, door Verwerker, te worden verwijderd.
5. De gegevens dienen tot 6 maanden na het einde van de overeenkomst beschikbaar te blijven, tenzij er sprake is van een situatie als bedoeld in lid 4 van dit artikel. Na 4 maanden zal Verwerker een signaal geven aan Opdrachtgever, dat de gegevens over 2 maanden worden vernietigd, tenzij Opdrachtgever wenst dat de gegevens dienen te worden bewaard.
6. Indien Verwerkeringsverantwoordelijke een verzoekt indient, zal Verwerker verklaren dat het wissen conform het bepaalde in lid 5 heeft plaatsgevonden tenzij er sprake is van een situatie als bedoeld in lid 4 van dit artikel. Indien Verwerker, na toestemming van Opdrachtgever, een subverwerker heeft ingeschakeld, zal Verwerker deze subverwerker op de hoogte stellen van de opdracht tot wissing en hem instrueren te handelen zoals hierin bepaald is.
7. Verwerker zal zich onthouden van het verrichte van andere handelingen, genoemd in artikel 1, tenzij anders overeengekomen in bijlage I.

Artikel 2: Naleving wet- en regelgeving

1. Verwerker zal bij enige verwerking van persoonsgegevens als in artikel 1 omschreven, handelen in overeenstemming met de Algemene Verordening Gegevensbescherming en overige van toepassing zijnde wet- en regelgeving aangaande gegevensbescherming.
2. Zowel de Opdrachtgever als de Verwerker geven elkaar inzage in de documentatie als bedoeld in artikel 30 AVG, indien van toepassing.

Artikel 3: Vrijwaring en aansprakelijkheid (maak keuze uit drie alternatieven)

Alternatief 1:
Opdrachtgever vrijwaart Verwerker voor alle aanspraken, behoudens opzet en/of grove schuld door Verwerker, bij schending van het gestelde bij of krachtens wet- en regelgeving aangaande gegevensbescherming of de uitvoering van deze overeenkomst.

Alternatief 2:
Verwerker vrijwaart Opdrachtgever voor alle aanspraken, behoudens opzet en/of grove schuld door Opdrachtgever, bij schending van het gestelde bij of krachtens wet- en regelgeving aangaande gegevensbescherming of de uitvoering van deze overeenkomst.

Alternatief 3:
Opdrachtgever vrijwaart Verwerker gelijk Verwerker Opdrachtgever vrijwaart voor alle aanspraken, behoudens opzet en/of grove schuld door Verwerker respectievelijk Opdrachtgever, bij schending van het gestelde bij of krachtens wet- en regelgeving aangaande gegevensbescherming of de uitvoering van deze overeenkomst.

Artikel 4: Beveiligingsmaatregelen, Compliance en incidenten

1 Verwerker zal, gelijk Opdrachtgever, passende technische en organisatorische maatregelen nemen, in stand houden, evalueren en indien nodig aanpassen en actualiseren om persoonsgegevens te beveiligen tegen verlies, diefstal, of tegen enige vorm van onrechtmatige verwerking. Deze maatregelen garanderen, rekening houdend met de aard, de omvang, de context en het doel van de verwerking, de stand van de techniek en de kosten van de tenuitvoerlegging, een passend beveiligingsniveau gelet op de waarschijnlijkheid en ernst uiteenlopende risico's die de verwerking en van te beschermen gegevens met zich meebrengen en voldoen aan het bepaalde in de richtsnoeren en artikel 32 AVG.

2 Verwerker stelt op verzoek van de Opdrachtgever alle informatie ter beschikking, die nodig is om nakoming van het bepaalde in lid 1 te kunnen aantonen.

3 Indien Verwerker in een andere lidstaat van de Europese Unie de gegevens van Opdrachtgever bewerkt of doet bewerken, zal zij dat doen of laten doen in overeenstemming met de wettelijk vereiste beveiligingsmaatregelen van de betreffende lidstaat.

4 Verwerker stelt Opdrachtgever in staat om op haar eerste, schriftelijke verzoek de getroffen maatregelen te inspecteren, met als doel na te gaan hetgeen in deze overeenkomst is bepaald.

5 Verwerker zal hieraan zijn medewerking verlenen en alle voor de audit relevante informatie tijdig ter beschikking stellen die nodig zijn om de nakoming van de in artikel 28 AVG neergelegde verplichtingen te kunnen aantonen.

6 Opdrachtgever zal in beginsel geen audit uitvoeren bij subverwerkers omdat de Verwerker hiervoor zelf volledig verantwoordelijk en aansprakelijk is.

7 De personen die een audit uitvoeren, zullen zich conformeren aan de beveiligingsprocedure zoals die bij Verwerker van kracht zijn. De kosten voor een audit komen voor rekening van Opdrachtgever, tenzij uit de audit blijkt dat Verwerker heeft gehandeld in strijd met deze overeenkomst of nagelaten heeft voldoende passende maatregelen te nemen rekening houdend met de stand van de techniek en de kosten van de tenuitvoerlegging, gelet op de risico's die de verwerking, de aard, de omvang, de context en het doel van de te beschermen gegevens met zich meebrengen.

8 De Opdrachtgever zal de audit beperkten tot hetgeen is vastgesteld in deze overeenkomst, voor de gegevensverwerkingen en de persoonsgegevens van Opdrachtgever. Gegevensverwerkingen die Verwerker voor andere Opdrachtgever uitvoert zijn van deze audit uitgesloten. Alle informatie waar Opdrachtgever kennis van krijgt tijdens de audit en die geen betrekking hebben op Opdrachtgever zal Opdrachtgever geheimhouden.

9 Indien Verwerker bij het verwerken van persoonsgegevens kennis krijgt van een inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens, die waarschijnlijk een risico inhoudt voor de rechten en vrijheden van de betrokkene, dan zal Verwerker onverwijld, edoch binnen 24 uur na ontdekking, Opdrachtgever daar van op de hoogte brengen, terwijl Verwerker in de tussentijd alle mogelijke technische en organisatorische maatregelen neemt om het beveiligingsincident te stoppen, te voorkomen en/of te herstellen. Verwerker verstrekt bij de melding informatie omtrent de aard van de inbreuk, de aard van de gelekte persoonsgegevens, de technische beschermingsmaatregelen en overige relevante feiten en omstandigheden die van belang zijn om te bepalen of de toezichthouder en/of de betrokkene geïnformeerd dienen te worden.

10 Verwerker zal Bijlage II melding datalek onverwijld volledig invullen en digitaal met de ingevulde contactpersonen naar Opdrachtgever versturen. Bijlage 2 toevoegen

11 Indien er gerede twijfel is of de inbreuk een waarschijnlijk risico inhoudt voor de rechten en vrijheden van betrokkene, dan meldt de Verwerker de inbreuk wel aan de Opdrachtgever, om deze in staat te stellen een eigen oordeel te vormen of een melding noodzakelijk is.

12 Verwerker documenteert alle inbreuken in verband met persoonsgegevens, ook de inbreuken die niet aan Opdrachtgever gemeld hoeven te worden. De documentatie bevat alle feiten omtrent de inbreuk, de gevolgen en de genomen corrigerende maatregelen. De documentatie wordt eens per kwartaal aan de Opdrachtgever verstrekt teneinde ervoor te zorgen dat Opdrachtgever in staat is deze te overleggen aan de Autoriteit Persoonsgegevens.

13 Indien er een verplichting bestaat een melding te doen aan de toezichthouder of om de betrokkenen te informeren zal dat uitsluitend worden gedaan door Opdrachtgever. Verwerker zal hierbij haar volstrekte medewerking en bijstand verlenen om aan deze verplichtingen te kunnen voldoen.

Artikel 5: Inschakeling subbewerkers binnen Europese Unie

1. Het is Verwerker niet toegestaan om in het kader van deze overeenkomst gebruik te maken van een subverwerker, tenzij Opdrachtgever hiertoe haar voorafgaande uitdrukkelijke schriftelijke toestemming heeft gegeven. Toestemming wordt hierbij verleend voor de in bijlage 1 genoemde subverwerkers.
2. Opdrachtgever kan nadere voorwaarden verbinden aan de inschakeling van een subverwerker bij de uitvoering van deze verwerkersovereenkomst.
3. De subverwerker biedt afdoende garanties met betrekking tot de toepassing van passende technische en organisatorische maatregelen opdat de verwerking aan het bepaalde van deze overeenkomst en de AVG voldoet.
4. Indien Verwerker een subverwerker heeft ingeschakeld, dan is Verwerker volledig aansprakelijk voor het nakomen van alle verplichtingen door deze subverwerker, maar niet voor subverwerkers waarvan de Opdrachtgever de Verwerker verplicht heeft om mee samen te werken, voor de werkzaamheden besloten in de opdracht van deze overeenkomst. Verwerker zal in een schriftelijke overeenkomst deze derde dezelfde verplichtingen opleggen als die voor hem uit deze overeenkomst voortvloeien, zodat ook de subverwerker gebonden wordt aan deze bepalingen.
5. Verwerker dient een lijst bij te houden van subverwerkers inclusief de uit te voeren taken.

Artikel 6: Inschakeling subverwerkers buiten Europese Unie

1. Indien Verwerker de persoonsgegevens buiten de Europese Unie wil verwerken, dan kan dit uitsluitend in landen, die door de Europese Commissie of de Minister van Justitie zijn aangemerkt als landen met een passend beschermingsniveau, of door aanvullende maatregelen een passend beschermingsniveau bieden.
2. De verwerking van persoonsgegevens buiten de Europese Unie kan uitsluitend na uitdrukkelijke voorafgaande schriftelijke toestemming van Opdrachtgever. Aan een dergelijke verwerking kunnen bovendien aanvullende voorwaarden worden gesteld.
3. Opdrachtgever verleent toestemming dat Verwerker de in bijlage 1 genoemde subverwerkers buiten de Europese Unie mag inschakelen.
4. De subverwerker biedt afdoende garanties met betrekking tot de toepassing van passende technische en organisatorische maatregelen opdat de verwerking aan het bepaalde van deze overeenkomst en de AVG voldoet.
5. Indien Verwerker een subverwerker heeft ingeschakeld, dan is Verwerker volledig aansprakelijk voor het nakomen van alle verplichtingen door deze subverwerker, maar niet voor subverwerkers waarvan de Opdrachtgever de Verwerker verplicht heeft om mee samen te werken, voor de werkzaamheden besloten in de opdracht van deze overeenkomst. Verwerker zal in een schriftelijke overeenkomst deze derde dezelfde verplichtingen opleggen als die voor hem uit deze overeenkomst voortvloeien, zodat ook de subverwerker gebonden wordt aan deze bepalingen.
6. Verwerker dient een lijst bij te houden van subverwerkers inclusief de uit te voeren taken.

Artikel 7: Geheimhoudingsplicht

1. Verwerker, haar personeel en door haar ingeschakelde derden zijn op basis van artikel 28 lid 3 onder b AVG verplicht tot geheimhouding met betrekking tot de persoonsgegevens waarvan zij kennisnemen of hebben kunnen nemen.
2. Verwerker verschaft enkel toegang tot de persoonsgegevens aan haar medewerkers en door haar ingeschakelde derden voor zover dit nodig is voor het verrichten van de door Opdrachtgever opgedragen gegevensverwerking.
3. Verwerker zal de personen die in dienst zijn, dan wel werkzaamheden ten behoeve van hem verrichten verplichten tot geheimhouding met betrekking tot de persoonsgegevens waarvan zij kennis kunnen nemen.
4. De geheimhoudingsplicht van Verwerker kan slechts worden doorbroken wanneer een wettelijk voorschrift verplicht om gegevens te verstrekken of de functionaris die is aangewezen door Opdrachtgever FUNCTIONARIS WEL INVOEGEN OP DEZE PLEK aan Verwerker de noodzaak tot mededeling heeft aangegeven.
5. Indien door een toezichthouder van Opdrachtgever inzage wordt gevraagd in de gegevensverwerking, dient Verwerker hieraan alle noodzakelijke medewerking te verlenen, om Opdrachtgever in staat te stellen om aan haar door toezichthouders opgelegde verplichtingen te voldoen.
6. De geheimhoudingsplicht geldt zowel tijdens als na afloop van de werkzaamheden en blijft ook na beëindiging van deze overeenkomst bestaan.
7. De Verwerker zal de Opdrachtgever op de hoogte stellen van ieder verzoek tot kennisneming, verstrekking of andere vorm van opvragen en mededeling van de persoonsgegevens, tenzij wetgeving deze kennisgeving om gewichtige redenen van algemeen belang verbiedt.

Artikel 8: Rechten van betrokkenen

1. Indien een betrokkene een van zijn rechten op grond van art. 15 tot en met 22 AVG inroept bij Verwerker, dan zal Verwerker dit verzoek onverwijld aan Opdrachtgever doorsturen.
2. Verwerker zal Opdrachtgever volledige en tijdige bijstand verlenen bij de uitoefening van diens plicht om verzoeken inzake uitoefening van de in lid 1 genoemde rechten te beantwoorden.

Artikel 9: Algemene voorwaarden & slotbepalingen

1. Op deze overeenkomst zijn geen algemene voorwaarden van toepassing. Het Nederlands recht is van toepassing. De bevoegde rechter is de rechter die bevoegd is op basis van de hoofdovereenkomst.
2. Indien in een andere overeenkomst tussen Opdrachtgever en Verwerker bepalingen zijn opgenomen die afwijken van hetgeen is bepaald in deze overeenkomst, prevaleert het bepaalde in deze overeenkomst.
3. Wijzigingen op deze overeenkomst zijn uitsluitend geldig indien deze tussen partijen schriftelijk zijn overeengekomen.
4. Deze overeenkomst treedt in werking op het moment dat de hoofdovereenkomst en heeft een looptijd die gelijk is aan die van de hoofdovereenkomst. Deze overeenkomst kan niet tussentijds worden opgezegd.

Aldus overeengekomen in tweevoud op [DATUM], te [PLAATS],

Opdrachtgever	**Verwerker**
Naam:	Naam:
Functie:	Functie:

Bijlage 1

NADER INVULLEN

Alle opsommingen zijn illustratief en dienen te worden aangepast aan de feitelijke situatie.

Werkzaamheden

De volgende werkzaamheden worden door de Verwerker uitgevoerd:

1. Het werven van persoonsgegevens via het concept .....;
2. Het voeren van een gegevensverwerking met de verzamelde persoonsgegevens;
3. Het verwerken van mutaties in de verzamelde persoonsgegevens;
4. Het uitvoeren van analyses en tellingen;
5. Het uitvoeren van selecties en deze plaatsen op een drager;
6. Panelbeheer;
7. Het maken van een back-up van de verzamelde persoonsgegevens;
8. Etc.
9. Etc.

Verwerker zal zich onthouden van het verrichte van andere handelingen dan de hierboven genoemde verwerkingen, zelfs niet wanneer deze in een zodanige vorm zijn gebracht dat ze niet meer herleidbaar zijn tot natuurlijke personen. Evenmin is Verwerker gerechtigd om de persoonsgegevens samen te voegen met andere bestanden van Verwerker, dan wel om de persoonsgegevens voor eigen of andere doeleinden te verwerken.

Persoonsgegevens

De Verwerker ontvangt hiervoor de volgende persoonsgegevens of categorieën van persoonsgegevens:

1. NAWTE;
2. Verrichte transacties;
3. Antwoorden op vragenlijst;
4. Etc.
5. Etc.

Bewaartermijnen

In afwijking van het bepaalde in artikel 1.4 tot en met 1.6 wordt de volgende bewaartermijn overeengekomen:

- ☐ geen afwijking
- ☐ volgende afwijking
  - invullen
  - invullen
  - invullen

Subverwerkers binnen Europese Unie

Opdrachtgever verleent toestemming voor de inschakeling van de volgende subverwerkers die binnen de Europese Unie gevestigd zijn:

Naam	Adresgegevens	Binnen EU	Verwerkingen
naam invullen	adres invullen	land invullen	omschrijving dienstverlening

Subverwerkers binnen Europese Unie

Opdrachtgever verleent toestemming voor de inschakeling van de volgende subverwerkers die binnen de Europese Unie gevestigd zijn:

Naam	Adres-gegevens	Buiten EU	Adequaatheids-maatregel (zoals Privacy Shield of Standard Contractual Clauses)	Verwerkingen
naam invullen	adres invullen	land invullen	invullen	omschrijving dienstverlening

Beveiliging

De Verwerker neemt op verzoek van de Opdrachtgever de volgende extra beveiligingsmaatregelen:

1. Bestanden worden uitgewisseld via een SFTP;
2. Etc.

Indien u werkzaam bent voor de overheid, dan kunt u worden geconfronteerd met deze beveiligingseisen. Zorg ervoor dat u hier goed kennis van neemt en zich afvraagt of u hier aan kunt voldoen.
Opdrachtgevers kunnen nadere beveiligingseisen stellen, bijvoorbeeld dat er wordt voldaan aan ISO 27001 of ISO 27002. Verwerker dient dan te bezien of aan deze eisen kan worden voldaan.

Indien de Opdrachtgever een overheidsorgaan is, dan kunnen deze van toepassing worden verklaard.

Arbit: de ARBIT zijn vooral bedoeld voor modale IT-inkopen door de overheid en niet zozeer voor grote en bijzondere IT-Projecten. Vaak kunnen opdrachten aan onderzoeksorganisaties niet als IT-inkopen worden gekwalificeerd. Een verwerkersovereenkomst blijft onverminderd van toepassing.
Arvodi: De Arvodi zijn Algemene Rijksvoorwaarden voor het verstrekken van opdrachten tot het verrichten van diensten. U dient zelf te beslissen of u als onderzoeksorganisatie Arvodi wenst te accepteren. Een verwerkersovereenkomst blijft onverminderd van toepassing.

Bijlage 2

MELDING DATALEK VERWERKER

Melding wordt gedaan door de directie van de verwerker aan opdrachtgever. Updates van het vragenformulier worden telkens zo snel mogelijk aan de opdrachtgever beschikbaar gesteld, genoemd aan het einde van dit formulier

Vragenformulier melding

0 Contactpersoon bij bewerker:

Vul onderstaande gegevens in:	
Naam:	
Functie:	
Mobiele telefoon:	
E-mailadres:	

1 Is dit een vervolg op een eerdere melding?

Kies een van onderstaande opties. Maak een keuze	
a) Ja	
b) Nee	

2 Van wanneer dateert de oorspronkelijke melding?

(Beantwoord deze vraag als u vraag 1 met ja hebt beantwoord). Invullen	
Datum:	

3 Wat is de strekking van de vervolgmelding?

(Beantwoord deze vraag als u vraag 1 met ja hebt beantwoord, kies een van de volgende opties). Maak een keuze	
a) Toevoegen of wijzigen van informatie betreffende de eerdere melding	
b) Intrekking van de eerdere melding	

4 Wat is de reden van intrekking?

(Beantwoord deze vraag als u bij vraag 3 hebt gekozen voor optie b). Invullen	
De reden van intrekking is:	

5 Geef een samenvatting van het incident waarop de inbreuk op de beveiliging van persoonsgegevens zich heeft voorgedaan.

6 Van hoeveel personen zijn persoonsgegevens betrokken bij de inbreuk?

Vul de aantallen in	
a) Minimaal: (vul aan)	
b) Maximaal: (vul aan)	

7 Omschrijf de groep mensen van wie persoonsgegevens zijn betrokken bij de inbreuk.

8 Wanneer vond de inbreuk plaats?

Kies een van de volgende opties: maak een keuze en vul in	
a) Op (datum)	
b) Tussen (begindatum periode en einddatum periode).	
c) Nog niet bekend	

Wanneer werd de inbreuk ontdekt?

Op (datum)

9 Wat is de aard van de inbreuk?

Reden, u kunt meerdere mogelijkheden kiezen	
a) Lezen (vertrouwelijkheid)	Ja/nee
b) Kopiëren	Ja/nee
c) Veranderingen (integriteit)	Ja/nee
d) Verwijderen of vernietigen (beschikbaarheid)	Ja/nee
e) Diefstal	Ja/nee
f) Nog niet bekend	Ja/nee

10 Om welk type persoonsgegevens gaat het? U kunt meerdere mogelijkheden aankruisen.

Type persoonsgegevens, u kunt meerdere mogelijkheden kiezen	
a) Naam-, adres- en woonplaatsgegevens	Ja/nee
b) Telefoonnummers	Ja/nee
c) E-mailadressen of andere adressen voor elektronische communicatie	Ja/nee
d) Toegangs- of identificatiegegevens (bijvoorbeeld inlognaam/ wachtwoord of klantnummer)	Ja/nee
e) Financiële gegevens (bijvoorbeeld rekeningnummer, creditcardnummer)	Ja/nee
f) Burgerservicenummer (BSN) of sofinummer	Ja/nee
g) Paspoortkopieën of kopieën van andere legitimatiebewijzen	Ja/nee
h) Geslacht, geboortedatum en/of leeftijd	Ja/nee
i) Bijzondere persoonsgegevens (Bijvoorbeeld ras, etniciteit, criminele gegevens, politieke overtuiging, vakbondslidmaatschap, religie, seksuele leven, medische gegevens).	Ja/nee. Zo ja welke
j) Overige gegevens, namelijk (vul aan)	

11 Welke gevolgen kan de inbreuk hebben voor de persoonlijke levenssfeer van de betrokkene?

Gevolgen, u kunt meerdere mogelijkheden kiezen	
a) Stigmatisering of uitsluiting	Ja/nee
b) Schade aan de gezondheid	Ja/nee
c) Blootstelling aan (identiteits-) fraude	Ja/nee
d) Blootstelling aan spam of phising	Ja/nee
e) Anders, namelijk (vul aan).	Ja/nee

12 Welke technische en organisatorische maatregelen heeft uw organisatie getroffen om de inbreuk aan te pakken en om verdere inbreuken te voorkomen?

13 Wanneer is het datalek gemeld aan de Verantwoordelijke/Opdrachtgever?

Invullen	
Datum en tijdstip:	
Contactpersoon Verantwoordelijke:	
Mededeling is gedaan per, maak keuze:	
a) Telefoon	
b) E-mail	
c) Formulier	
d) Anders, namelijk	

14 Zijn de persoonsgegevens, versleuteld, gehasht of op een andere manier onbegrijpelijk of ontoegankelijk gemaakt voor onbevoegden?

Kies een van de opties en vul waar nodig aan	
a) Ja	
b) Nee	
c) Deels, namelijk (vul aan):	

15 Als de persoonsgegevens geheel of deels onbegrijpelijk of ontoegankelijk zijn gemaakt, op welke manier is dit dan gebeurd?
(Beantwoord deze vraag als u bij vraag 14 gekozen heeft voor optie a of optie c. Als u gebruik heeft gemaakt van encryptie, licht dan ook de wijze van versleutelen toe).

16 Is naar uw mening deze melding compleet?

Selecteer een van de onderstaande opties, maak uw keuze	
a) Ja, de vereiste informatie is verstrekt en er is geen vervolgmelding nodig.	
b) Nee, er komt later een vervolgmelding met aanvullende informatie over deze inbreuk.	

Afsluitend:

Naam ondertekenaar Verwerker:	
Plaats:	
Datum:	
Handtekening:	

Contactpersoon bij Verwerker:

Naam:	
Functie:	
Mobiele telefoon:	
E-mail:	

Formulier met spoed beschikbaar stellen aan:

Contactpersoon bij Opdrachtgever:

Naam:	
Functie:	
Mobiele telefoon:	
E-mail:	

Het formulier is door Opdrachtgever ontvangen op:

Datum en tijdstip: