Privacyreglement

Eigenaar: functionaris gegevensbescherming
Versie: januari 2024
Evaluatie: juni 2024

Inhoud

1. Inleiding

Visie

Centraal bij ENA staat de ouder wordende mens, die als volwaardig burger en als (participerend) lid van de samenleving ondersteuning nodig heeft bij zijn/haar vragen op het terrein van wonen, welzijn én zorg.
ENA heeft de ambitie om ouderen midden in het leven te laten staan. Daarmee bedoelen wij dat ouderen, ook wanneer zij aangewezen zijn op onze diensten of zorg, hun normale leven zoveel mogelijk voortzetten. Dit heeft consequenties voor de wijze waarop we zorg en diensten verlenen, namelijk cliëntgericht en bewust van de kwaliteit die de zorg en dienstverlening voor de cliënten biedt. Dit geldt ook voor de huisvesting van onze cliënten.
Dit vraagt van de medewerkers een werkhouding die is gericht op het ingaan op vragen en wensen.

Om die professionele zorg te kunnen bieden beschikken medewerkers en vrijwilligers over privacygevoelige informatie. ENA heeft beleid opgesteld om op een zorgvuldige manier om te gaan met privacygevoelige informatie. Dat kunnen gegevens van cliënten, contactpersonen, medewerkers, vrijwilligers en andere relaties zijn.
In dit document leest u op welke wijze ENA de zorgvuldige omgang met persoonsgegevens organiseert, toetst en meldt bij de Autoriteit Persoonsgegevens (AP) wanneer er iets mis is gegaan, kortom hoe ENA de Algemene Verordening Gegevensbescherming (AVG) toepast.

Wetgeving (AVG)

Het doel van de AVG is het beschermen van persoonsgegevens van medewerkers, cliënten, bewoners, vrijwilligers en leveranciers.
De belangrijkste uitgangspunten in de verordening zijn:

- Er moet een wettelijke basis zijn om persoonsgegevens te verwerken (zie hoofdstuk 2).
- Persoonsgegevens mogen niet langer bewaard worden dan voor het doel waarvoor deze gegevens oorspronkelijk verwerkt werden.
- Dataminimalisatie; er mogen niet meer gegevens worden gebruikt dan noodzakelijk is voor het doel dat bereikt moet worden.
- Privacy by design; dit betekent dat bij de inrichting van producten en/of diensten zo vroeg mogelijk aandacht besteed wordt aan het beschermen van persoonsgegevens en dataminimalisatie.
- Privacy bij default; dit betekent dat gebruikers zelf de mogelijkheid hebben om persoonsgegevens te delen en/of op te slaan en/of af te staan. Zij hebben inzicht in datgene wat van hen vastligt.

De toepassing van de AVG binnen ENA

De principes uit de AVG zijn verankerd in procedures, werkwijzen en protocollen van ENA. De AVG is onderdeel van het dagelijks handelen. De AVG vraagt doorlopende aandacht voor bewustwording van iedereen op alle fronten. In de audits wordt het voldoen aan de AVG getoetst.

Functionaris gegevensbescherming

In het kader van de AVG heeft ENA een functionaris gegevensbescherming (FG) aangesteld. De taken van de FG binnen ENA zijn:

- Aanspreekpunt zijn voor de Autoriteit Persoonsgegevens (AP).
- Adviseren en ondersteunen op het gebied van privacybeleid en bescherming van persoonsgegevens.
- Bijhouden van een verwerkingsregister.
- Het bijhouden van een datalekregister en het verrichten van eventuele externe meldingen, als een datalek bij de AP.
- Advisering bij het uitvoeren van een DPIA.
- Toezien op het correct toepassen en naleven van de AVG en bewustzijn hierover creëren binnen de organisatie.

2. Verwerken van persoonsgegevens

Inleiding

Onder persoonsgegevens wordt verstaan alle informatie over een geïdentificeerde of identificeerbare persoon. Het gaat niet alleen om naam-, adres- en woonplaatsgegevens van een natuurlijke persoon, maar ook om informatie die direct of indirect te herleiden zijn tot een natuurlijk persoon. Naast algemene persoonsgegevens zijn er ook bijzondere persoonsgegevens. Dit zijn gegevens waaruit bijvoorbeeld ras, of etnische afkomst, religieuze of levensbeschouwelijke overtuiging, medische gegevens of het lidmaatschap van een vakbond blijken.

In dit hoofdstuk worden eerst de regels uit de AVG toegelicht: wat is het verwerken van gegevens, welke rechten hebben individuen bij het verwerken van persoonsgegevens, hoe is die verwerking binnen ENA georganiseerd bij repeterende verwerkingen en eenmalige verwerkingen, gevolgd door een overzicht van wettelijke bewaartermijnen en het privacystatement van ENA.

Verwerken van persoonsgegevens

De AVG geeft een ruime omschrijving wat verstaan moet worden onder de verwerking van persoonsgegevens. Het verzamelen, vastleggen, opslaan of verspreiden van gegevens, maar ook het ordenen of wissen van gegevens. Het begrip ‘verwerking’ is dusdanig breed dat vrijwel elke wijze van verwerking onder dit begrip valt.
ENA mag niet zomaar gegevens verwerken. In het kader van de AVG is de verwerking minimaal gebaseerd op 1 van de 6 grondslagen voor verwerking die in de wet genoemd worden. Dit zijn:

- Toestemming van de betrokken persoon. Toestemming houdt in dit geval in “elke vrije, specifieke, geïnformeerde en ondubbelzinnige wilsuiting waarmee de betrokkene door middel van een verklaring of een duidelijke actieve handeling, hem betreffende, verwerking van persoonsgegevens aanvaardt” (artikel 4 lid 11 AVG)
- De gegevensverwerking is noodzakelijk voor de uitvoering van een overeenkomst.
- De gegevensverwerking is noodzakelijk voor het nakomen van een wettelijke verplichting.
- De gegevensverwerking is noodzakelijk ter bescherming van de vitale belangen.

- De gegevensverwerking is noodzakelijk voor de vervulling van een taak van algemeen belang of uitoefening van openbaar gezag.
- De gegevensverwerking is noodzakelijk voor de behartiging van de gerechtvaardigde belangen.

Alle verwerkingen van persoonsgegevens binnen ENA berusten op minimaal een van de zes grondslagen.

Rechten van personen waarvan gegevens worden verwerkt

ENA heeft t.a.v. de verwerking van gegevens van cliënten, medewerkers, stagiaires en vrijwilligers op grond van de wet verschillende verplichtingen. Het gaat om:

- De verplichting informatie te verschaffen over de verwerkingen, dat wordt geregeld in de zorgovereenkomsten met cliënten, arbeidsovereenkomsten met medewerkers, overeenkomsten met vrijwilligers en het privacystatement. Tevens worden alle verwerkingen bijgehouden in het verwerkingsregister.
- De verplichting zich te kunnen verantwoorden over de verwerkingen die uitgevoerd worden. Dat doet ENA op basis van een actueel verwerkingsregister.
- Betrokkenen hebben recht op inzage. Een betrokkene kan vragen om een overzicht van gegevens die over hem verzameld worden.
- Betrokkenen hebben recht op correctie als de gegevens feitelijk onjuist zijn, onvolledig zijn, of niet ter zake doen voor het doel waarvoor ze verzameld werden.
- Betrokkenen hebben het recht op vergetelheid. Dit recht geldt alleen wanneer de verwerking niet meer nodig is voor de doeleinden waarvoor de gegevens werden verzameld, de betrokkene de toestemming intrekt, de betrokkene bezwaar maakt tegen de verwerking, de verwerking onrechtmatig is, de wettelijke bewaartermijn verstreken is, de betrokkenen jonger dan 16 jaar is en zijn gegevens via een website of app heeft achtergelaten.

Verwerking binnen ENA

Een betrokkene van wie persoonsgegevens worden verwerkt binnen ENA moet door ENA worden geïnformeerd over de categorieën van persoonsgegevens die verwerkt worden en het doel daarvan. Dit betekent dat ENA een overzicht moet hebben. Het overzicht wordt bijgehouden in het verwerkingsregister. In het verwerkingsregister heeft ENA vastgelegd welke gegevens verwerkt worden van cliënten, medewerkers en vrijwilligers. De volgende gegevens zijn opgenomen:

- Betreffende deelproces: zoals het op de wachtlijst plaatsen van een cliënt, of het bijhouden van verzuim
- Wie betrokken zijn bij dit deelproces
- Wat de gegevensbron is die gebruikt word
- Waar de gegevens worden opgeslagen (digitaal en/of papier)
- Wie er bij de gegevens kunnen
- Om welke categorie persoonsgegevens gaat het
- Wat de wettelijke grondslag voor het mogen verwerken van deze gegevens is
- Wat het doel is van de vastlegging van deze gegevens
- Hoe lang deze gegevens bewaard worden
- Welke veiligheidsmaatregelen genomen worden om de gegevens te beschermen

Binnen ENA zijn afspraken gemaakt om dit verwerkingsregister actueel te houden. Deze taak ligt bij de FG.

Afgesloten contracten voor verwerking van persoonsgegevens

ENA moet in het kader van verschillende repeterende processen persoonsgegevens verwerken waarbij derden betrokken zijn. Denk bijvoorbeeld aan het verwerken van salarisgegevens om tot een correcte betaling te komen, of het gebruik van het digitale cliëntendossier dat bij een externe leverancier is gekocht die ook als helpdesk functioneert. ENA heeft met al deze leveranciers duidelijk afspraken gemaakt over de verwerking van deze gegevens en deze afspraken vastgelegd in verwerkersovereenkomsten.

DPIA

ENA verwerkt als zorginstelling gegevens. Het verwerken van gegevens met een repeterend karakter ligt vast in het verwerkingsregister. Bij veranderingen in processen, aanschaf van nieuwe systemen etc. waarbij persoonsgegevens betrokken zijn is het van groot belang om voorafgaand aan die (grootschalige) verwerking van gegevens de mogelijke privacy risico 's daarvan in kaart te brengen. Het gaat dan vooral om evaluatie van de oorsprong, de aard, het specifieke karakter en de ernst van deze privacy risico 's. Het instrument daarvoor is de DPIA. Op basis daarvan kunnen maatregelen worden genomen om de risico 's te verkleinen. ENA kan door het uitvoeren van een DPIA vroegtijdig inzicht krijgen op de belangrijkste risico's wanneer aanpassingen in processen nodig zijn of herontwerp van systemen. Op deze manier wordt invulling gegeven aan vereiste principes 'privacy by design en privacy by default'.

Wettelijke bewaartermijnen

Cliënten

Gegevens	Wettelijk bewaartermijn	Te rekenen vanaf
Gegevens over de behandeling van cliënten en de verpleging en de verzorging in dat kader	Minimaal 20 jaar (artikel art. 454 lid 3 Wgbo)	De laatste wijziging in het dossier
Toelichting: In de Wgbo is bepaald dat medische gegevens die in het dossier zijn opgenomen voor een periode van twintig jaar bewaard moeten worden. De periode van twintig jaar gaat volgens de wet in op het tijdstip waarop de laatste wijziging in het dossier heeft plaatsgevonden. Uitzondering: Medische gegevens mogen langer bewaard indien nodig om de cliënt goede zorg te blijven geven. De cliënt kan ENA ook vragen om zijn gegevens langer te bewaren dan de wettelijke termijnen. Dat kan van belang zijn bij erfelijke aandoeningen of bij juridische procedures. De cliënt kan vragen om zijn gegevens eerder te vernietigen. Dat kan ook voordat de wettelijke termijnen zijn verstreken. Dit geldt niet als cliënt gedwongen was opgenomen in een psychiatrisch ziekenhuis. Verantwoordelijke naleven termijn: Klantadvies		

Gegevens van cliënten in verzorgingshuizen en verpleeghuizen over huisvesting en voorzieningen	Maximaal 5 jaar (artikel 17 Vrijstellingsbesluit WBP)	Einde zorgverlening
Toelichting: Het gaat hier niet om de zorggegevens maar *uitsluitend* om gegevens die gebruikt worden voor doeleinden als huisvesting en voorzieningen. Zoals de NAW-gegevens van de cliënt en zijn contactpersoon, zijn bankrekeningnummer en de contactgegevens van zijn huisarts. Verantwoordelijke naleven termijn: Klantadvies		
Medicatiegegevens van cliënten	20 jaar	De laatste wijziging in het dossier
Toelichting: Het actueel medicatieoverzicht is onderdeel van het dossier van de arts en apotheker en van het zorgdossier en volgt in beginsel de wettelijke bewaartermijn van de Wgbo (20 jaar). Verantwoordelijke naleven termijn: Klantadvies		
Toedienlijsten medicatie	2 jaar	De einddatum van de betreffende toedienlijst
Toelichting: Deze termijn geldt niet indien op een bepaald moment bij een cliënt zich een relevante substantiële bijzonderheid heeft voorgedaan (bijv. ziekenhuisopname na verkeerde dosis medicatie) die, naar het oordeel van de behandelend arts, het langer bewaren van de toedienlijsten rechtvaardigt c.q. noodzakelijk maakt. Verantwoordelijke naleven termijn: Teamleider zorg van de locatie		
Gegevens over behandeling van Wzd-cliënten (onvrijwillige zorg)	20 jaar	Het einde onvrijwillige zorg
Verantwoordelijke naleven termijn: Klantadvies		
Gegevens voor het huren van een woning Verantwoordelijke naleven termijn: nvt	2 jaar	Einde huurcontract

Medewerkers

Gegevens	Wettelijk bewaartermijn	Te rekenen vanaf
Gegevens medewerkers indien fiscaal relevant Verantwoordelijke naleven termijn: Personeelsadviseur	Maximaal 7 jaar (art. 52 Wet Rijksbelastingen art. 8 Douanewet)	Einde dienstverband
Loonbelastingverklaring Verantwoordelijke naleven termijn: Personeelsadviseur	Maximaal 5 jaar (art. 6 Loonadministratiebesluit)	Einde dienstverband
Kopie identiteitsbewijs Verantwoordelijke naleven termijn: Personeelsadviseur	Maximaal 5 jaar op grond van Wet Identificatieplicht, art. 23 a Uitvoeringsregeling loonbelasting)	Einde dienstverband
Overige gegevens van medewerkers zoals arbeidsovereenkomsten, ontwikkelgesprekken (voorheen functioneringsgesprekken) Verantwoordelijke naleven termijn: Personeelsadviseur	Maximaal 2 jaar	Einde dienstverband
Uitzondering: (tenzij er sprake is van een juridisch geschil of een kans hierop bestaat (vanwege een arbeidsrechtelijk geschil)		
Gegevens sollicitanten (brieven, verslagen, tests) Verantwoordelijke naleven termijn: Personeelsadviseur	Maximaal 4 weken	Einde procedure
Uitzondering: tenzij kandidaten “in portefeuille’ worden gehouden. Met toestemming van sollicitant: maximaal 1 jaar		

Cameratoezicht

Gegevens	Wettelijk bewaartermijn	Te rekenen vanaf
Camerabeelden in openbare ruimten	Maximaal 4 weken	Vastlegging van de beelden
Toelichting: Langer is geoorloofd indien de beelden bewijsmateriaal zijn in een strafrechtelijk onderzoek, of redelijkerwijs verwacht kan worden dat de beelden een rol kunnen spelen in een strafrechtelijk onderzoek. Verantwoordelijke naleven termijn: Projectleider Facilitair & Inkoop		

Privacystatement

ENA heeft een privacystatement opgesteld. Het privacystatement is een document waarin ENA beknopt, transparant en op begrijpelijke wijze uitlegt hoe zij omgaat met persoonsgegevens. Het privacystatement is zowel van toepassing op de papieren als elektronische verwerking van gegevens. Het privacystatement is gepubliceerd op de website van ENA.

3. Afspraken cliënten, medewerkers stagiaires vrijwilligers

Inleiding

ENA heeft verschillende verplichtingen zoals de wettelijke verplichting om personen te informeren over de categorieën persoonsgegevens die zij vastlegt en ook uit te leggen op grond waarvan zij dat doet (de wettelijke grondslagen). Voor minderjarigen gelden andere regels. Ook dient ENA informatie te verschaffen wanneer daarom gevraagd wordt. Op welke wijze daaraan invulling gegeven wordt is in dit hoofdstuk te vinden.

Cliënten

Alle cliënten die bij ENA komen wonen tekenen een zorgovereenkomst. In deze zorgovereenkomst wordt uitgelegd dat er persoonsgegevens worden verwerkt om aan de afspraken in de overeenkomst te kunnen voldoen.

In de informatie voor nieuwe cliënten wordt verder verwezen naar het privacystatement dat te vinden is op de website. Daarnaast tekenen alle cliënten een toestemmingsformulier voor additionele toestemmingen die buiten de overeenkomst om geregeld moeten worden.

Medewerkers, stagiaires en vrijwilligers

In de arbeidscontracten van medewerkers van ENA is opgenomen dat medewerkers zich bewust zijn van het privacystatement en daar ook naar moeten handelen. Daarnaast is ook een alinea over geheimhouding opgenomen.
Voor vrijwilligers is er een aparte vrijwilligersovereenkomst.

Naast het verwerken van deze persoonsgegevens vraagt ENA aan nieuwe medewerkers, stagiaires en vrijwilligers expliciet toestemming voor de volgende verwerkingen;

- Uitvoeren van (tevredenheids-) onderzoeken
- Correspondentie vanuit de organisatie
- Gebruik van foto's voor interne communicatie doeleinden
- Gebruik van foto's voor externe communicatie doeleinden

Medewerkers, stagiaires en vrijwilligers geven ENA toestemming onder de volgende voorwaarden:

- Als de gegevens niet meer noodzakelijk zijn zal ENA de gegevens niet meer registreren dan wel verwijderen (volgens de wettelijke termijnen).
- Medewerkers, stagiaires en vrijwilligers mogen de toestemming op elk moment intrekken. In sommige gevallen kan het intrekken van de toestemming consequenties hebben voor het dienstverband.

Afwijkende regels voor minderjarigen

Indien een minderjarige medewerker in dienst komt wordt op het arbeidscontract, behalve een handtekening van de medewerker, ook een handtekening van de ouder of wettelijke voogd vereist. De salarisadministratie en de leidinggevende die de medewerker in dienst neemt zijn voor uitvoering van deze afspraak verantwoordelijk. Dit geldt voor jongeren van 16 jaar of jonger.

4. Afspraken binnen ENA in omgaan met privacygevoelige informatie

Inleiding

ENA onderschrijft het belang om de beschikbaarheid, integriteit en vertrouwelijkheid van de informatie en de informatievoorziening te beschermen. Hulpmiddelen daarbij zijn: de geheimhouding vanuit de beroepsgroep, het opgestelde ICT-gedragsprotocol, de wijze waarop ENA de verantwoordelijkheden t.a.v. het privacyreglement heeft belegd, archivering van e-mails en documenten, printen naar openbare printers, het gebruik van loggegevens en beeldmateriaal en het buiten gebruik stellen apparatuur dat persoonsgegevens kan bevatten. De verschillende onderdelen worden in deze paragraaf toegelicht

ICT gedragsprotocol

ENA stelt haar medewerkers ICT-middelen en -voorzieningen zoals computers met software daarop, internettoegang en e-mail ter beschikking voor het uitoefenen van de functie. Om de beschikbaarheid, integriteit en vertrouwelijkheid van de informatie en de informatievoorziening te beschermen, is er een Gedragscode ICT vastgesteld. Beleid en technische maatregelen alleen zijn niet voldoende om de goede werking van de ICT-middelen en -voorzieningen te waarborgen. Ongewenst gebruik kan grote hinder en schade opleveren. Dit protocol voorziet in een aantal richtlijnen en geboden voor verantwoord gebruik van de ICT-middelen door de medewerker.

Uitgangspunten

Zakelijk gebruik. De beschikbaar gestelde ICT-middelen zijn primair bedoeld voor zakelijk gebruik. Beperkt privégebruik is toegestaan voor zover dit niet indruist tegen de gestelde regels, niet storend is voor de overeengekomen werkzaamheden en geen extra kosten voor ENA tot gevolg heeft.
Vertrouwelijkheid. Medewerkers moeten zich er van bewust zijn dat men met vertrouwelijke bedrijfsgegevens te maken heeft. Het gebruik van ICT-middelen mag eventuele vertrouwelijkheid of gevoeligheid van gegevens niet schenden of strijdig zijn met wettelijke of contractuele beperkingen.
Privacy. Op zowel het gebruik als controle op het gebruik van ICT-middelen is het Privacyreglement van ENA van toepassing.
Overlast voorkomen. Het gebruik van internet en e-mail is aan bepaalde regels en beperkingen gebonden. Hierbij gelden ook de gangbare omgangsvormen bij communicatie.
Zorgvuldigheid. De medewerker dient zorgvuldig om te gaan met de beschikbaar gestelde ICT-middelen en zich te houden aan de gestelde regels.

Het ICT-gedragsprotocol is niet vrijblijvend. De instructies, geboden en verboden uit dit protocol gelden voor alle medewerkers van ENA. Overtreding van dit ICT-gedragsprotocol kan leiden tot sancties.

Definities

- *ICT-middelen* – De door ENA ter beschikking gestelde hardware, software en netwerkfaciliteiten, evenals de voorzieningen t.b.v. elektronisch data- en spraakverkeer. Waaronder: desktop- en laptopcomputers en de daarop geplaatste programmatuur, internettoegang, e-mail, maar ook printer, scanner, PDA (elektronische agenda), (mobiele) telefoon en smart device.
- *Beveiligingsincident* – Een incident waarbij de reputatie van ENA op het spel zou kunnen staan of de bedrijfsvoering buitenproportioneel kan worden verstoord, met het risico dat de beschikbaarheid, integriteit en vertrouwelijkheid van informatie wordt aangetast. Bijvoorbeeld het verliezen van een mobiele telefoon, het kwijtraken van een USB-stick etc.
- *Internetgebruik* – Het uitwisselen of doorgeven van gegevens en/of berichten via e-mail, het bezoeken van internetsites, het binnenhalen (downloaden) van gegevens alsmede het binnenhalen van software en/of het gebruiken van software vanaf internet.
- *Smart device* – Een draadloos apparaat, niet zijnde een pc, dat zich kenmerkt door computerfunctionaliteit, waarop applicaties beschikbaar zijn, waarmee via internet of wifi-informatiesystemen van ENA kunnen worden benaderd. Bijvoorbeeld mobiele telefoon, smartphone of tablet.

Privacy en controle

- De inhoud van een e-mail is persoonlijk van aard. Alleen de medewerker kan anderen toegang tot de inhoud van zijn/haar e-mailverkeer geven. Voor het verlenen van ondersteuning is het in bepaalde situaties nodig dat de medewerker toegang verleent tot zijn of haar mailbox aan de afdeling ICT. In zulke gevallen zal de medewerker deze toegang verlenen.

- Het gebruik van applicaties, e-mail- en internet wordt op permanente basis centraal gemonitord en gelogd. Deze monitoring heeft in eerste aanleg een technische oorsprong om de werking van de systemen te kunnen beoordelen.

Gebruik van de ICT-middelen

- Het gebruik van de ICT-middelen door de medewerker is in de eerste plaats ten behoeve van het vervullen van zijn taak of functie. Beperkt privégebruik is toegestaan, indien dit niet storend is voor de overeengekomen werkzaamheden en geen extra kosten voor ENA met zich meebrengt.
- ENA heeft de bevoegdheid een medewerker de mogelijkheid tot het gebruik van ter beschikking gestelde ICT-middelen te ontzeggen.
- Installatie van software op ICT-middelen geschiedt uitsluitend door de (intern of extern) systeem- of applicatiebeheerder.
- Het installeren van software zonder een geldige licentie is verboden.
- Mede met het oog op beheer van licenties en de ondersteuning van de gebruikers kan de afdeling ICT controles uitvoeren ten aanzien van geïnstalleerde software.
- Tablets, laptops, telefoons en smartphones mogen nooit onbeheerd achterblijven. Indien deze meegenomen moeten worden in de auto, geldt dat deze niet zichtbaar (indien je de auto verlaat zonder deze middelen mee te nemen) in een afgesloten auto achter mogen blijven.
- In geval van schade, vermissing of diefstal van ICT-middelen dient de leidinggevende en de afdeling ICT direct geïnformeerd te worden.
- Reparaties aan en opening van apparatuur mag uitsluitend door de afdeling ICT uitgevoerd worden. Bij het verlaten van de werkplek dient de medewerker handmatig de schermvergrendelmodus te activeren (toetsen combinatie CTR+ALT+END).
- Afhankelijk van de locatie van een werkplek (kantoor, thuis, vergaderruimte, appartement cliënt), gaat mobiel computergebruik gepaard met andere risico's, waarvoor medewerkers bijbehorende beveiligingsmaatregelen dienen te treffen.
- Medewerkers mogen lokaal geen bestanden opslaan.

Thuiswerken

Indien een medewerker thuis werkt dient hij/zij zich bewust te zijn van het feit dat gewerkt wordt met vertrouwelijke documenten/dossiers. De medewerker zorgt en is verantwoordelijk voor de veiligheid van de (elektronische) documenten en houdt zich ook thuis aan het bij ENA geldende privacystatement en de afspraken m.b.t. het veilig omgaan met privacygevoelige informatie.

Internet

- Internet wordt door medewerkers alleen zakelijk gebruikt, samenhangend met de werkzaamheden die de medewerker bij ENA verricht. Internetsites waarvan het vermoeden kan bestaan dat bezoek ervan mogelijk nadelige gevolgen voor de ICT-middelen tot gevolg kan hebben, mogen niet worden bezocht. Voor alle duidelijkheid: het is verboden internetsites te bezoeken die pornografisch en/of racistisch en/of ander kwetsend of aanstootgevend materiaal bevatten.
- ENA kan internetsites voor gebruik blokkeren. In dit geval zal een melding verschijnen dat de betreffende pagina is geblokkeerd.
- ENA kan de doorgifte van bepaalde typen bestanden blokkeren. Het gaat om bestanden die de capaciteit van de internetverbinding onnodig kunnen belasten

(bijvoorbeeld mp3 - files, streaming media etc.) of schadelijk kunnen zijn voor ENA.
- Het downloaden van software vanaf internet en het gebruiken van software vanaf internet (SaaS) is slechts toegestaan met uitdrukkelijke toestemming van de afdeling ICT.
- Bij internetgebruik dient de medewerker zorg te dragen dat de rechten van derden (zoals auteursrechten, merkenrechten) niet worden geschonden.
- Indien op een internetsite naam, bedrijfsgegevens en/of e-mailadres moeten worden achtergelaten om gegevens op te vragen of te verkrijgen, dan zal de medewerker dat uitsluitend doen als er een zakelijke reden voor is. Ook zal de medewerker in dat geval aangeven dat die gegevens niet voor andere doeleinden gebruikt mogen worden. Bedrijfsgevoelige informatie zal nooit worden doorgegeven of op een internetsite worden achtergelaten.

Intranet
Intranet van ENA wordt als informatievoorziening gebruikt voor medewerkers. De regels die van toepassing zijn op internet gelden ook voor het gebruik van intranet.

Social media
Richtlijnen voor gebruik van social media:
- Medewerkers, die actief zijn op social media (blogs/vlogs, wiki's of sociale netwerken als bijvoorbeeld LinkedIn, YouTube, Flickr, Twitter, Facebook etc.), gaan verstandig en zorgvuldig om met deze media en zij plaatsen geen vertrouwelijke of interne informatie.
- Bloggen/vloggen over het werk(-en) bij ENA gebeurt altijd eerlijk en transparant en met gebruik van de echte naam. Men dient aan te geven waar en in welke functie men werkzaam is en of men schrijft op persoonlijke titel of namens de organisatie.
- Medewerkers reageren niet op gesignaleerde negatieve berichten over ENA, maar melden deze bij hun leidinggevende.

E-mail
- E-mail wordt in beginsel uitsluitend zakelijk gebruikt om het risico op imagoschade voor ENA tot een minimum te beperken.
- Indien privacygevoelige informatie gedeeld moet worden is communicatie per systeem (ECD, HR-software), telefoon of beveiligd e-mailen noodzakelijk.
- ENA kan doorgifte van e-mailberichten blokkeren wanneer zij mogelijk virussen bevatten of gegevens bevatten waarvan de verspreiding of verzending onwenselijk is.
- Voor e-mailverkeer gelden dezelfde regels en beleefdheidsnormen als ten aanzien van telefonische en niet-elektronische communicatie.
- Oproepen van derden om plaatjes, post, koopaanbiedingen, kettingbrieven of goedbedoelde (virus)waarschuwingen algemeen binnen ENA te verspreiden dienen te worden genegeerd. Het is verboden dergelijke oproepen zelf te verspreiden.
- In geval van viruswaarschuwingen moet (uitsluitend) de afdeling ICT worden geïnformeerd.
- Het is verboden dreigende, seksueel intimiderende en/of racistische taal te gebruiken dan wel te verspreiden.

- ENA stelt indien voor het werk noodzakelijk een e-mailbox ter beschikking. De medewerker is zelf verantwoordelijk voor het regelmatig opschonen van zijn mailbox.

Beveiligingsbeleid

- Op het gebruik van e-mail (zowel inkomend als uitgaand), intranet en internet zijn de geheimhoudingsverplichtingen voortvloeiend uit de arbeidsovereenkomst tussen de medewerker en ENA van toepassing
- Indien nodig ontvangt een medewerker van de afdeling ICT een gebruikersnaam, wachtwoord en instructies om het systeem van ENA te benaderen. Instructies van de afdeling ICT met betrekking tot wachtwoorden en de eventuele wijziging daarvan dienen te worden opgevolgd.
- De leidinggevende van de betreffende medewerker is verantwoordelijk voor het, in overeenstemming met het functieprofiel, bepalen van de juiste toegangsrechten en ziet erop toe dat eventuele functie- of taakwijzigingen van medewerkers direct tot uiting komen in hun toegangsrechten.
- Medewerkers nemen beveiligingsgewoonten in acht bij het kiezen en gebruiken van hun wachtwoord(en), waardoor wachtwoorden moeilijk te raden zijn. Na gebruik loggen zij uit. Zij veranderen het wachtwoord indien de vertrouwelijkheid van het wachtwoord wordt betwijfeld. Zij worden hierin ondersteund door de techniek. Medewerkers zijn in beginsel, tot het tegendeel blijkt, persoonlijk verantwoordelijk voor misbruik van hun account.
- Alle medewerkers houden hun accountgegevens waaronder het wachtwoord en pincode geheim. Zij gebruiken hun persoonlijke account en uitgegeven autorisaties alleen zelf en staan niet toe dat anderen onder hun account kunnen inloggen. Opgeslagen wachtwoorden en pincodes van medewerkers en derden zijn in geen geval leesbaar door anderen dan de betrokkene zelf. Het is verboden een wachtwoord mede te delen aan anderen dan de afdeling ICT.
- Indien de medewerker in het bezit is van USB-sticks, cd- en dvd-roms die niet meer worden gebruikt, dan dient deze de betreffende informatiedragers leeg te maken en te vernietigen (bijvoorbeeld doorknippen dvd- of cd-rom en weggooien).
- Het is niet toegestaan om vertrouwelijke informatie buiten het ENA-netwerk te verzenden of op te slaan. Onder vertrouwelijke informatie wordt verstaan alle informatie die als zodanig is aangeduid of informatie waarvan de medewerker weet of zou behoren te weten dat deze vertrouwelijk is. Dit geldt voor e-mail (hotmail, gmail, etc.), het gebruik van diensten voor het verzenden van grote bestanden (Dropbox, WeTransfer, etc.) en andere diensten waarbij ENA-informatie buiten het Ena-netwerk wordt opgeslagen (Prezi, Googledrive, etc.).
- Het is toegestaan informatie in de vorm van e-mail op een smartphone of tablet (zakelijk of privé) op te slaan. Als er informatie (bijv. e-mail) op een smartphone of tablet staat, is het ICT-gedragsprotocol van toepassing en moet op het device een minimale vorm van beveiliging worden toegepast, bestaande uit een wachtwoord. Dit wordt door het e-mailsysteem afgedwongen. Medewerkers die uit hoofde van hun functie met persoonsgegevens te maken hebben mogen deze alleen opslaan op een device van ENA.
- Iedere (ingehuurde) medewerker meldt beveiligingsincidenten bij de FG. Deze legt de meldingen vast in een register. Het gaat om incidenten waarbij persoonsgegevens betrokken zijn en waarbij de reputatie van ENA op het spel zou kunnen staan, de bedrijfsvoering substantieel wordt verstoord, de

beschikbaarheid, integriteit en vertrouwelijkheid van informatie(middelen) wordt aangetast of goederen worden gestolen.
- Alle zakelijke gegevens en informatie, inclusief e-mailberichten, gegenereerd, gedragen of ontvangen door ICT-middelen van ENA zijn eigendom van ENA.
- Ter beschikking gestelde ICT-middelen mogen zonder voorafgaande en schriftelijke toestemming van ENA niet aan derden in gebruik worden gegeven. Evenmin mogen een of meer kopieën van programmatuur aan derden worden verstrekt.

Verantwoordelijkheden ENA

In onderstaande tabel worden de uitgangspunten beschreven van de rollen en taken van personen die zich bezighouden met informatiebeveiliging- en privacybeleid en van personen die via toegekende autorisatie persoonsgegevens verwerken.

Niveau	Wie/rollen	Hoe verantwoordelijkheid/taken	Wat realiseren/vastleggen
Richtinggevend Strategisch	Bestuurder	• Eindverantwoordelijk • Informatiebeveiliging en privacy beleidsvorming m.b.t. vastleggen en actief uitdragen • Verantwoordelijk voor het zorgvuldig en rechtmatig verwerken van persoonsgegevens • Evaluatie • Organisatie van Informatie en Privacy beleid • (Crisis)communicatie bij grootschalige incidenten	• Informatie en Privacy beleid • Basismaatregelen • Functionaris gegevensbescherming benoemen • Privacyreglement vaststellen • Inzet security bij grootschalig datalek
Sturend Tactisch	Financial Controller ICT beheerder	• Inhoudelijk verantwoordelijk voor informatiebeveiliging • Advies aan bestuurder • Verantwoordelijk voor hantering normen en organisatie van toetsen (audit) • Evalueren beleid informatiebeveiliging	• Beleid en protocollen informatiebeveiliging (zoals gedragscode ICT.) • Bewustwordingsactiviteiten • Informatie aan betrokkenen (cliënten, familie, medewerkers, vrijwilligers) • Toestemming gebruik foto's etc.
	Strategisch beleidsadviseur	• Evalueren privacybeleid • Schrijven en beheren van processen, richtlijnen en procedures ter ondersteuning van de uitvoering	• Beleid en protocollen informatiebeveiliging, privacy AVG (zoals protocol DPIA, protocol datalekken, privacy beleid etc.)
	Functionaris Gegevensbe-scherming (FG)	• Toezicht naleving AVG • Advies privacy/AVG • Register datalekken en melding bij AP • Verwerkingsregister • Privacyreglement en -statement • Bewustwording AVG in organisatie	• Advies over privacygerelateerde zaken/beleid • Privacyreglement en -statement • Controle op naleving verwerkersovereen-komsten • Bewustwordingsactiviteiten
	Aandachthouders AVG, waaronder Beleidsmedewerker	• Risicoanalyse (met FG) • Toegangsbeleid tot systemen in samenwerking	• Inventariseren waar persoonsgegevens van cliënten, medewerkers,

	Medewerker organisatie en beleid Intern ICT-beheerder Salarisadministratie Cliëntadministratie Automatiseringscommissie	met manager en goed laten keuren door bestuurder • Toezien op juiste toegangen tot systemen • Samen met intern ICT-beheerder de toegangsrechten regelmatig beoordelen en controleren	contactpersonen en vrijwilligers terecht komen • Toegangsmatrix informatiesystemen en netwerk • Informatie- en privacy beleid onder de aandacht brengen en houden van collega's
Uitvoerend Operationeel	FG Financial controller ICT-beheerder Medewerker Leidinggevende	• Incidentafhandeling • Technisch aanspreekpunt voor incident • Uitvoeren van taken volgens afspraken en richtlijnen • Preventief onderhoud aan servers • Verantwoordelijk voor het op een juiste manier omgaan met persoonsgegevens en privacygevoelige informatie • Communicatie, zorgen dat medewerkers, vrijwilligers op de hoogte zijn van het beleid • Onderwerp op de agenda plaatsen • Toezien op de naleving van het beleid • Voorbeeldfunctie • Implementatie van maatregelen • Rapporteren over voortgang informatie- en privacy beleid/ incidenten in dashboard	Communiceren, informeren en toezien op naleving • Informatiebeveiliging en Privacy beleid algemeen • Hoe omgaan met cliënten dossiers • Wie mogen wat zien • Gedragscode ICT • Mediawijs maken • Zorgen voor back-ups • Zorgen voor veilige opslag van gegevens

Archivering

Voor het bewaren van persoonsgegevens gelden wettelijke termijnen (zie hoofdstuk 2, wettelijke bewaartermijnen). Om aan die richtlijnen te kunnen voldoen en daadwerkelijk alle persoonsgegevens te vernietigen na afloop van de bewaartermijn of indien een persoon daarom verzoekt, zijn binnen ENA afspraken gemaakt over het bewaren van persoonsgegevens.

Basisafspraken:

- Cliëntgegevens worden zoveel mogelijk bewaard in het ECD. Zowel de cliënt (vertegenwoordiger) als de zorgmedewerkers en cliënt administratie hebben toegang tot het dossier.
- Medewerker gegevens worden zoveel mogelijk vastgelegd in de HR-software. Zowel medewerkers als leidinggevenden, HR en salarisadministratie hebben toegang tot het systeem.
- Vrijwilligersgegevens worden zoveel mogelijk vastgelegd in SWO office (access database).

E-mail versturen en archiveren:

- Voor het veilig versturen van externe e-mail met persoonsgegevens wordt ZorgMail gebruikt.
- Het onderling (tussen ENA e-mailadressen) versturen van e-mails die persoonsgegevens bevatten is dat akkoord, indien men zich houdt aan de archiveringsafspraken.
- Leidinggevenden, personeelsfunctionaris en medewerkers salarisadministratie en P&O gebruiken de mogelijkheid “versturen bericht” in selfservice naar een medewerker indien de inhoud van het bericht persoonsgegevens betreft.
- Zorgmedewerkers gebruiken (indien mogelijk) een berichtenmodule in het ECD voor het versturen van berichten aan cliënten (eerste contactpersonen), die persoonsgegevens van betreffende cliënt bevatten.
- Externe e-mails die ontvangen worden en die persoonsgegevens bevatten mogen niet als archief bewaard worden in de mail. Cliëntinformatie of medewerkerinformatie moet verwerkt worden in de daartoe aangewezen systemen.
- E-mails met persoonsgegevens mogen niet onbeperkt bewaard worden. Dit geldt voor zowel in- als externe e-mails. En zowel voor inkomende als uitgaande e-mails. Dit betekent dat iedere medewerker met een eigen e-mailadres binnen ENA zowel de uitgaande als inkomende e-mailbox in ieder geval één keer per jaar moet opschonen.
- Persoonsgegevens van sollicitanten mogen slechts één maand bewaard worden (na afloop van de procedure). Dit betekent dat digitale sollicitaties opgeslagen worden in een map op de lokale schijf gedurende de sollicitatieprocedure. De leden van de sollicitatiecommissie hebben toegang tot die map. Na afronding van de procedure wordt de map van de lokale schijf verwijderd door de personeelsfunctionaris. Cv’s en dergelijke worden niet per e-mail doorgestuurd.
- Er is een uitzondering op het bewaren van gegevens van sollicitanten. Indien sollicitanten expliciet toestemminggeven mogen de gegevens maximaal één jaar bewaard worden. Hiervoor wordt een centrale map op de lokale schijf gebruikt waar de HR-functionaris en medewerker organisatie en beleid toegang toe hebben.

Documenten

Het kan voor de uitvoering van het werk binnen ENA noodzakelijk zijn om persoonsgegevens vast te leggen buiten het ECD of de HR-software. Om ervoor te zorgen dat we daar zorgvuldig mee omgaan worden de volgende afspraken gemaakt:

- Het vastleggen van persoonsgegevens is van tijdelijke aard en dient een organisatie specifiek doel. Bijvoorbeeld in het kader van een organisatieverandering, het verzamelen van gegevens t.b.v. een raadpleging (cliënten-, medewerker-, vrijwilligers-, mantelzorgers), specifiek project, afleggen van verantwoording aan de overheid en/of accountant.
- De documenten worden bij elkaar opgeslagen in een centrale map waar alleen betrokkenen toegang toe hebben. Er wordt niets in persoonlijke mappen, dan wel decentraal opgeslagen.
- Aan het eind van het traject wordt bepaald in hoeverre vastgelegde gegevens bewaard moeten worden. Indien deze bewaard moeten worden, worden deze zoveel mogelijk in systemen bewaard. Indien dat niet mogelijk is wordt vastgelegd waar deze vastgelegd zijn en waarom, zodat de bewaartermijn in

acht genomen kan worden en personen “vergeten” kunnen worden indien zij daar om vragen.

Printen naar openbare printers

Vanuit verschillende werkplekken binnen ENA kan geprint worden op gedeelde printers. De printers staan in een afzonderlijke ruimte waar meerdere personen toegang toe hebben. Om te voorkomen dat bij printers papieren liggen met persoonsgegevens staan alle computers standaard ingesteld op beveiligd printen. De gebruiker kan de printer uitsluitend in werking zetten door op het apparaat een persoonlijke code in te toetsen.

Gebruik loggegevens en beeldmateriaal

Binnen ENA worden verschillende systemen gebruikt. In deze systemen worden handelingen van personen vastgelegd. Het gaat om de volgende systemen:

- Camerasysteem bij de ingang en uitgang van het gebouw. Registreert continu personen die het pand inkomen en/of verlaten. Doel: herkenning, signalering, identificatie en preventie. In het gebouw hangen bordjes met cameratoezicht. De beelden worden automatisch overschreven als de disk vol is.
- Sleutelkast. Om een sleutel te kunnen pakken dient ingelogd te worden met een pincode. De kast legt vast welke tag gebruikt wordt om de sleutel te pakken en terug te hangen. De kast registreert datum, tijdstip en sleutelnummer.
- Het elektronisch cliëntendossier (ECD) registreert alle inlogs, naam, tijdstip en welke pagina’s bezocht worden.
- Mobiele telefoons. Bij het telecombedrijf is op te vragen per nummer hoe vaak en waar naartoe gebeld is, hoeveel data verbruikt en welke pagina’s bezocht zijn.
- Interne telefoons. Per telefoon is uit te lezen waar naar toe is gebeld, zowel in- als extern.
- Oproepsysteem. Wanneer een cliënt een oproep plaatst, is uit te lezen hoe lang het duurt voor de oproep beantwoord wordt en welk toestel gebruikt wordt bij beantwoording.

In het dagelijks werk wordt niets met de mogelijkheid om gegevens die gelogd zijn te lezen gedaan. Bij incidenten kunnen de gegevens uitgelezen worden en gebruikt worden. Bijvoorbeeld bij het analyseren van een incident, om op zoek te gaan naar een mogelijk onbekende die het pand binnen is gegaan, bij een extreem hoge telefoonrekening na te vragen wat de oorzaak is etc. Omdat het gaat om persoonsgegevens is zorgvuldigheid en het voorkomen van willekeur vereist. De volgende afspraken worden gemaakt:

- Een mogelijk incident wordt gemeld bij een lid van ENA Kompas.
- De ENA Kompas-leden kunnen, op basis van het incident, de ICT-medewerkers opdracht geven gelogde gegevens op te zoeken en aan hen aan te bieden.
- De gegevens worden in opdracht van het ENA Kompas-lid geanalyseerd. Op basis van de analyse wordt besloten de gegevens al dan niet te gebruiken.
- Indien de gelogde gegevens gebruikt worden t.b.v. de oplossing van het incident worden de collega’s van ENA Kompas geïnformeerd.

Buiten gebruik stellen apparatuur die persoonsgegevens kan bevatten

Binnen ENA wordt gewerkt met verschillende apparaten. Op een aantal apparaten worden persoonsgegevens vastgelegd. Denk daarbij aan:

- Smartphone
- Tablet
- Computer
- Laptop
- Digitale camera
- Servers

Wanneer de apparatuur buiten gebruik wordt gesteld, gelden de volgende afspraken:

- Alle apparaten worden ingeleverd bij ICT.
- De ICT/TD-medewerker beoordeelt de buitengebruikstelling. Indien daadwerkelijk buiten gebruik, afgeschreven en niet meer bruikbaar dan gelden de volgende regels:
    - De ICT-medewerker herstelt bij smartphones en tablets de fabrieksinstellingen en zorgt ervoor dat deze vernietigd worden.
    - Voor computers en laptops geldt dat de harde schijf uit het apparaat gehaald wordt. De harde schijf wordt onklaar gemaakt (m.b.v. een hamer). De verschillende onderdelen (elektrische apparaten) worden afgevoerd naar de stort.
    - Digitale camera, het geheugen wordt verwijderd en leeggehaald. Vervolgens wordt het geheugen vernietigd. De camera wordt afgevoerd via de stort (elektrische apparaten).
    - Servers worden leeg gemaakt en afgevoerd naar de stort.

5. Wat als het mis gaat

Ondanks alle afspraken die ENA maakt om op een zorgvuldige wijze met persoonsgegevens om te gaan kunnen er in het werk fouten gemaakt worden, waardoor persoonsgegevens terecht kunnen komen bij “onbevoegden”. (Voorbeelden zijn: op een bureau ligt een verslag van een verzuimgesprek en een ander dan de betrokkene of leidinggevende ziet het verslag, er wordt een e-mail die persoonsgegevens bevat naar de verkeerde persoon gestuurd, iemand raakt een onbeveiligde laptop van ENA kwijt).

Bij ENA worden dit soort fouten in kaart gebracht door middel van het digitaal invullen van het meldformulier en deze te sturen aan de FG (of diens vervanger bij vakantie of afwezigheid). Alle beveiligingslekken inclusief genomen acties worden door de FG vastgelegd in het register datalekken en de leidinggevende bespreekt dit 4x per jaar met het betrokken ENA Kompas-lid.

De AVG kent 2 soorten “fouten”:

- Datalek: Een beveiligingsincident waarbij persoonsgegevens verloren zijn gegaan of als onrechtmatige verwerking van de persoonsgegevens redelijkerwijs niet kan uitsluiten.
- Beveiligingslek: Een gebeurtenis waarbij de mogelijkheid bestaat dat de vertrouwelijkheid, integriteit of beschikbaarheid van informatie of informatie verwerkende systemen in gevaar is of kan komen. Voorbeelden van

beveiligingsincidenten zijn besmettingen met virussen en/of malware, pogingen om ongeautoriseerd toegang te krijgen tot informatie of systemen (hacken) of het ongeautoriseerd kunnen lezen van een verslag.

Datalekken moeten binnen 72 uur door de FG aan de AP worden gemeld. Voor het volledige protocol datalekken.