Privacybeleid Tûmba

Inwerkingtreding 1 juni 2022

Deel I. Persoonsgegevens en het doel van het bewaren van persoonsgegevens

1.1 Onder persoonsgegevens wordt verstaan:
   A. Direct identificerende gegevens; informatie waaruit de identiteit van iemand te herleiden is.
   B. Indirect identificerende gegevens; informatie die niet direct over een persoon gaat, maar wel naar een persoon te herleiden zijn.
   C. Bijzondere persoonsgegevens/omstandigheden; gevoelige informatie over het privéleven van de betrokkene(n).

1.2 Onder identiteit wordt verstaan: de voor- en achternaam, leeftijd, geslacht en gegevens over de woonplaats.

1.3 De klachtbehandelaar is verplicht zich te houden aan het geheimhouden van de persoonsgegevens van cliënt.

1.4 Daarnaast is de klachtbehandelaar verplicht om zich in te spannen voor de eerbiediging van het privéleven van cliënt.

1.5 Onder de eerbiediging van het privéleven van cliënt wordt verstaan: De verplichting op geheimhouding van iemands godsdienst, levensovertuiging, politieke gezindheid, ras, geslacht, burgerlijke staat, leeftijd, handicap of chronische ziekte, arbeidsomstandigheden of welke grond dan ook.

1.6 De persoonsgegevens worden alleen onder klachtbehandelaars en stagiaires van de afdeling Klachtbehandeling besproken en/of uitgewisseld. Zij hebben een geheimhoudingsplicht.

1.7 Onder klachtbehandeling wordt verstaan: Het registreren van de benodigde gegevens voor het landelijke registratiesysteem, om zo een overzicht te krijgen van de aard en omvang van de discriminatievoorvallen, en de behandeling van de discriminatiemelding door een procedure op te starten; waarmee wordt bedoeld dat er contact wordt gezocht met partijen voor het afhandelen van de discriminatiemelding.

1.8 De benodigde persoonsgegevens worden voor het volgende doel bewaard: een effectieve en transparante klachtbehandeling, zodat de klachtbehandelaar de wederpartij(en) alsook

andere betrokkenen van de discriminatiemelding op de hoogte kan houden over de identiteit van cliënt en van alle omstandigheden van de discriminatieklacht, zolang dit in het belang is voor de behandeling van de discriminatiemelding.

1.9 Persoonsgegevens mogen alleen worden verwerkt om het vastgestelde doel te bereiken. De klachtbehandelaar moet dan ook kunnen verantwoorden met welk doel hij/zij bepaalde persoonsgegevens heeft bewaard.

1.10 Voor het registreren en doorzetten van een melding, moet de melder te allen tijde een volwassene zijn. Dit houdt in dat hij/zij minimaal achttien jaar oud moet zijn. Op het moment dat het slachtoffer/melder een minderjarige betreft, moet de procedure van klachtbehandeling met zijn/haar ouder(s)/voogdij worden behandeld.

Deel II. Anonieme melding

1.11 Een anonieme melding is toegestaan, maar in het dergelijk geval is het niet te allen tijde mogelijk om een klacht door te zetten.

1.12 Met het doorzetten van een klacht wordt verstaan: naar aanleiding van de discriminatiemelding het opnemen van contact met partijen voor de behandeling van de melding.

1.13 De klachtbehandelaar heeft de vrijheid om te beoordelen of een anonieme melding doorgezet kan worden. Indien mogelijk, houdt de klachtbehandelaar de anonieme melder hiervan op de hoogte.

1.14 Een anonieme melding wordt ten minste geregistreerd, mits de postcode of woonplaats bekend is.

Deel III. Wettelijke taak; Wet gemeentelijke antidiscriminatievoorzieningen (Wga); geen toestemmingsvereiste; Algemene Verordening Persoonsgegevens (AVG)

1.1 De verwerking van (in)directe identificeerbare persoonsgegevens is alleen rechtmatig indien de verwerking noodzakelijk is om te voldoen aan een wettelijke verplichting die op de verwerkingsverantwoordelijke rust (artikel 6 AVG). De wet legt deze taak op aan Tûmba, zie hiervoor artikel 2, eerste lid, onderdeel b, van de Wga. Hierdoor kan Tûmba zonder toestemming deze benodigde persoonsgegevens van cliënten opvragen, registreren en bewaren.

1.2 De verwerking van bijzondere omstandigheden van persoonsgegevens is rechtmatig indien de verwerking noodzakelijk is om redenen van zwaarwegend algemeen belang, op grond van Unierecht of lidstatelijk recht (artikel 9 AVG). Discriminatie is verboden bij nationale wetgeving. Tûmba heeft als wettelijke taak: het registreren, voorkomen en bestrijden van discriminatie en bijstand te verlenen, zie hiervoor artikel 2, eerste lid, onderdeel a en b, van de Wga. Omdat de taakuitvoering in de nationale wet geregeld is en discriminatie verboden is bij wet, voert Tûmba een taak uit van zwaarwegend algemeen belang. Hierom mag Tûmba ook zonder toestemming van belang zijnde bijzondere persoonsgegevens (omstandigheden) vastleggen.

1.3 Cliënten hebben echter ook rechten als het gaat om hun (bijzondere) persoonsgegevens, zie hiervoor deel V, VI en VII.

Deel IV. Opvragen, verwerken, bewaren en vernietigen persoonsgegevens

1.1 (Persoons)gegevens en (de omstandigheden van) de discriminatiemelding worden in het registratiesysteem verwerkt en bewaard.
1.2 Onder het registratiesysteem valt: ADV-net.
1.3 De opgeslagen persoonsgegevens/privacygevoelige gegevens van cliënt moeten vanaf het moment van de melding alleen relevant zijn voor de registratie of behandeling van de klacht. Het opslaan van gegevens dat voor een effectieve en transparante klachtbehandeling er niet aan toe doet, is niet toegestaan; gelet op artikel 1.8 en 1.9 van deel I.
1.4 Ingevolge de statuten en de wettelijke taak is het opvragen en het bewaren van de volgende gegevens van cliënten noodzakelijk voor een transparante klacht(behandeling): initialen, achternaam, postcode, telefoonnummer en/of e-mailadres. In het geval er meer (persoons)gegevens nodig zijn, moet de klachtbehandelaar dit in het belang van de klachtbehandeling kunnen verantwoorden.
1.5 Ingevolge de statuten en de wettelijke taak is het opvragen en het bewaren van de volgende gegevens van wederpartij(en) noodzakelijk voor een transparante klacht(behandeling): initialen, achternaam, postcode, straatnaam en huisnummer, e-mailadres en/of telefoonnummer. In het geval er meer gegevens nodig zijn, moet de klachtbehandelaar dit in het belang van de klachtbehandeling kunnen verantwoorden.
1.6 Voor het bewaren van de straatnaam en huisnummer van cliënt alsook van de wederpartij(en) wordt zoveel mogelijk afgezien, tenzij correspondentie via de post noodzakelijk wordt geacht.
1.7 Indien de melding over de discriminatiegronden ras of nationaliteit gaat, mogen ook de nationaliteit en het ras van cliënt worden opgevraagd en bewaard voor de landelijke cijfers en een effectieve en transparante klachtbehandeling.
1.8 Indien de melding over discriminatie op grond van geloofsovertuiging gaat, geldt hetzelfde als bij artikel 1.7 en mag ook de religie van cliënt worden opgevraagd en bewaard.
1.9 Indien de melding over discriminatie op grond van geslacht gaat, geldt hetzelfde als bij artikel 1.7 en mag ook het geslacht van cliënt worden opgevraagd en bewaard.
1.10 Indien de melding over leeftijdsdiscriminatie gaat, geldt hetzelfde als bij artikel 1.7 en mag ook de leeftijd van cliënt worden opgevraagd en bewaard.
1.11 Indien de artikelen 1.7, 1.8, 1.9 en 1.10 van toepassing zijn, wordt het doel hiervan aan cliënt beargumenteerd, mits cliënt hierom vraagt.
1.12 Voor uitsluitend registratie van een melding is alleen de postcode of woonplaats van cliënt voldoende.
1.13 Alle persoonsgegevens die door cliënt niet desgevraagd aan Tûmba worden verstrekt, mag de klachtbehandelaar bewaren voor de klachtbehandeling, tenzij de informatie overbodig is voor een effectieve en transparante klachtbehandeling. De klachtbehandelaar moet dit kunnen verantwoorden.
1.14 Alle gegevens van cliënten worden vanaf het moment van binnenkomst van de melding gedurende vijf jaar bewaard. Hierna worden zij vernietigd. Het procesgang van vernietigen staat in het Protocol Databeveiliging van Tûmba, zie artikel 1.1 van deel IX.

Deel V. Informatieverstrekking aan de cliënt

1.1 Cliënten worden door middel van het Protocol Behandeling meldingen discriminatie[1] te allen tijde op de hoogte gebracht over de registratie en bewaring van hun persoonsgegevens en het doel daarvan.
1.2 Voor het doorzetten van een klacht, indien dit plaatsvindt door middel van correspondentie met de wederpartij(en) of derden, en voor het overleggen van (bijzondere) persoonsgegevens van cliënt aan deze partijen, moet aan cliënt te allen tijde om toestemming worden gevraagd. Dit vindt plaats door middel van het machtingsformulier.[2]
1.3 Cliënt heeft desgevraagd altijd het recht om te weten hoe lang zijn gegevens worden opgeslagen (bewaartermijn), het recht op dataportabiliteit, het recht over wie de ontvangers zijn van de persoonsgegevens en over de identiteit van Tûmba.

Deel VI. Recht van inzage en correctie

1.1 Cliënt heeft te allen tijde het recht op inzage wat betreft zijn/haar papieren en digitale dossiers en het recht van correctie, waaronder de bewaarde persoonsgegevens.
1.2 Op dit recht kan enkel een beroep worden gedaan indien cliënt fysiek aanwezig is op het kantoor van Tûmba.
1.3 De klachtbehandelaar mag het recht van inzage van cliënt niet beperken of negeren, tenzij de informatie betrekking heeft op privacygevoelige gegevens van de wederpartij of derden, waarbij het niet noodzakelijk wordt geacht dat cliënt hiervan op de hoogte moet worden gebracht voor een effectieve en transparante klachtbehandeling.

Deel VII. Recht van vergetelheid

1.1 Cliënt heeft te allen tijde het recht van vergetelheid (verwijdering) of het recht van verzet voor de bewaring van bepaalde (privacygevoelige) gegevens.
1.2 De klachtbehandelaar mag het recht van vergetelheid of het recht van verzet van cliënt niet negeren maar wel beperken, indien dit recht een verstoring is van een effectieve of transparante klachtbehandeling, of een verstoring van de wettelijke taak van Tûmba.

Deel IIX. Recht van registratie voor landelijke cijfers

1.1 Indien de melder een bezwaar heeft op de registratie/bewaring van zijn melding, kan hij zich niet met succes beroepen op de verwijdering van deze registratie. De klachtbehandelaar kan te allen tijde een melding registreren, mits de postcode of woonplaats bekend is. In dit geval mag de klachtbehandelaar geen enkel andere irrelevante gegevens van melder opslaan, waardoor de identiteit van melder te herleiden

[1] Bijlage 1: Werkwijze en stappenplan klachtbehandeling Art.1 MN
[2] Bijlage 2: Het machtigingsformulier

is. Wel mag de klachtbehandelaar andere relevante, privacygevoelige gegevens opslaan om de discriminatiemelding te voorzien van een transparante en overzichtelijke casus.

Deel IX. Informatieverzoeken

1.1 Indien een informatieverzoek binnenkomt, mag iedere medewerker van Tûmba de gegevens van de verzoeker opvragen, registreren en bewaren. De gegevens en informatie die te allen tijde verwerkt moeten worden zijn: naam, postcode, waar verzoeker tot behoort, het verzoek, het aanpak en de resultaat. Dit is vereist in het kader van een transparante overzicht van de jaarlijkse binnengekomen informatieverzoeken.

Deel X. Databeveiliging

1.1 De beveiliging van het dataverkeer vindt uitsluitend plaats door middel van het Protocol Databeveiliging 2018.[3]

Deel XI. Datalekken

1.1 Indien er een datalek plaatsvindt, wordt het Protocol Datalekken nagestreefd.[4]

Deel XII. Beveiliging van de website

1.1 De beveiliging van de website wordt door een externe systeembeheerder bewerkstelligd. Het netwerk –telefoon en internet- wordt beheerd door Telpa Telecom. De beheerder voert updates uit, voor zover dat nodig wordt geacht voor het realiseren van een website in optima forma. Op het moment dat er een update moet gebeuren, een (vermoeden van een) aanval plaatsvindt, of iets dergelijks van soortgelijke aard geschied, ontvang de beheerder een melding en voorkomt hij mogelijke schade.

Met opmerkingen [AS1]: Checken bij Harry hoe dit is vastgelegd - zijn deze documenten beschikbaar?

En is de websitebouwer ook onze 'systeembeheerder'? Hoe is dat georganiseerd?

Met opmerkingen [AS2R1]: Telpa Telecom beheerd ons netwerk. Er in week 28 een mail naar hen verstuurd om de documenten op te vragen.

Deel XIII. Beveiliging van de server

1.1 De beveiliging van de server is onder controle van Telpa Telecom, waarmee een verwerkersovereenkomst is afgesloten. De beheerder controleert voortdurend de algemene gezondheid van de server, schrijfruimte en de verdere vereisten voor een veilige server. Indien er een probleem optreedt, zoals een (vermoeden van een) aanval op de server, krijgt de beheerder hierover per direct een melding. In dat geval vindt er (uit voorzorgmaatregel) een blokkering plaats en wordt de server opnieuw geüpdatet en beveiligd.

1.2 Voor gasten en medewerkers zijn verschillende wifi-netwerken beschikbaar in verband met het waarborgen van de veiligheid van de server.

Met opmerkingen [AS3]: De 'externe systeembeheerder': wie is dat? Hoe is dit overeengekomen, wat staat erover op papier? De verwerkersovereenkomst dus.

Met opmerkingen [AS4R3]: In week 28 uitgevraagd aan Telpa. De verwerkersovereenkomst moet bij onze AVG-documenten komen te staan

Deel XIV. Het contactformulier op de website

Met opmerkingen [AS5]: Nieuw artikel ingevoerd

[3] Bijlage 3: Protocol Databeveiliging 2018
[4] Bijlage 4: Protocol Datalekken 2018

1.1 Het contactformulier op de website is de externe ingang voor het stellen van vragen, het aanvragen van de nieuwsbrief en het aanvragen van trainingen;
1.2 Bezoekers van de website worden aldaar steeds verwezen naar het contactformulier;
1.3 De mails uit het contactformulier komen binnen in de mailbox info@tumba.nl;
1.4 Bovenaan het contactformulier wordt expliciet verwezen naar het privacy protocol waarin beschreven staat dat de gegevens van diegene worden bewaard op het moment dat hij/zij zich inschrijft en met welk doel dit wordt bewaard;
1.5 Het doel luidt het volgende: bewaren van persoonsgegevens (naam en e-mailadres) voor eventuele beantwoording van de (aan)vraag;
1.6 De bewaarde gegevens mogen nimmer voor andere doeleinde gebruikt worden, tenzij daar toestemming voor is gevraagd en gegeven.

Deel XV. Nieuwsbrieven

1.7 De nieuwsbrief wordt verstuurd door middel van de mail;
1.8 De nieuwsbrief wordt alleen verstuurd naar personen of instanties die zich hebben aangemeld voor de nieuwsbrief;
1.9 Partijen kunnen zich door middel van het contactformulier inschrijven voor de nieuwsbrief.
1.10 Indien iemand, anders dan middels het inschrijfformulier, zich wil inschrijven voor de nieuwsbrief, moet aan diegene om toestemming worden gevraagd voor het bewaren van zijn gegevens en met welk doel. Diegene moet dan expliciet een akkoord geven;
1.11 De bewaarde gegevens en de toestemmingen worden in een overzicht behouden.
1.12 Op elk nieuwsbrief staat expliciet dat uitschrijven te allen tijde mogelijk is. De bewaarde gegevens worden dan onmiddellijk vernietigd.

Met opmerkingen [AS6]: GOED CHECKEN hoe de de nieuwsbrief staat vermeld op de website, en hoe dat gaan aangegeven.

Met opmerkingen [AS7R6]: "Wil je de nieuwsbrief in je mail ontvangen? Meld je dan hier aan! + vermelding van regels"

Met opmerkingen [AS8R6]: * bovenstaande doorgegeven aan Harry

Deel XVI. Aanvraag trainingen

1.1 Op de website staat een overzicht van de trainingen en wordt de mogelijkheid geboden deze aan te vragen via het contactformulier en de algemene contactgegevens (emailadres en telefoonnummers);

1.2 Indien iemand, anders dan middels het contactformulier, een aanvraag voor een training wil indienen, moet aan de indiener om toestemming worden gevraagd voor het bewaren van zijn gegevens en met welk doel. De indiener moet dan expliciet een akkoord geven;

1.3 De bewaarde gegevens en de toestemmingen worden in een overzicht bijgehouden.

1.4 Na een periode van ten hoogste vijf jaren na de aanvraag worden de gegevens vernietigd.

Deel XVII. Klachtenprocedure

1.1 Indien een persoon of een melder een klacht heeft over het optreden van Tûmba , kan deze klager hierover te allen tijde een klacht indienen.
1.2 Allereerst dient een klacht, zoals benoemt in lid 1.1 van dit deel, intern ingediend te worden. De directeur zal deze klacht in behandeling nemen, onderzoeken en naar aanleiding van de resultaten van het onderzoek een terugkoppeling doen aan de klager. Indien de indiener het niet eens is met het oordeel van de directeur, kan de klachtencommissie van Tumba aangeschreven worden. Deze klachtencommissie bestaat uit twee bestuursleden van Tumba en een externe onafhankelijke deskundige.
1.3 De interne klachtenprocedure staat op de website van Tûmba.
1.4 Indien de klager niet tevreden is met het resultaat van de interne klachtenprocedure, zoals benoemt in lid 1.2 van dit deel, kan de klacht voorgelegd worden aan de Externe Klacht Commissie (EKC) van Discrimatie.nl. De klacht wordt door een externe klachtenraad behandeld. Zij geven vervolgens hun oordeel over de klacht aan de klager aan Tûmba door. De procedure van de externe klachtenprocedure is te vinden op de website van Tûmba.
1.5 Indien naar voren komt dat Tûmba niet naar behoren heeft gehandeld, wordt er samen met de klager een doeltreffende oplossing gezocht.

Deel XVIII. Werving en selectie

Met opmerkingen [AS9]: Hier formuleren hoe we omgaan met de gegevens van sollicitanten

1.1 Sollicitatiegegevens worden binnen vier weken na afwijzing vernietigd.

1.2 Tûmba kan de sollicitant toestemming vragen de sollicitatiegegevens gedurende een half jaar te bewaren ten behoeve van eventuele toekomstige passende vacatures.

1.3 Voor overige richtlijnen ten behoeve van de verwerking en het bewaren van sollicitatiegegevens verwijzen we naar de Sollicitatiecode van de Nederlandse Vereniging voor Personeelsmanagement & Organisatieontwikkeling (NVP).

Deel XVIV. Functionaris voor gegevensbescherming

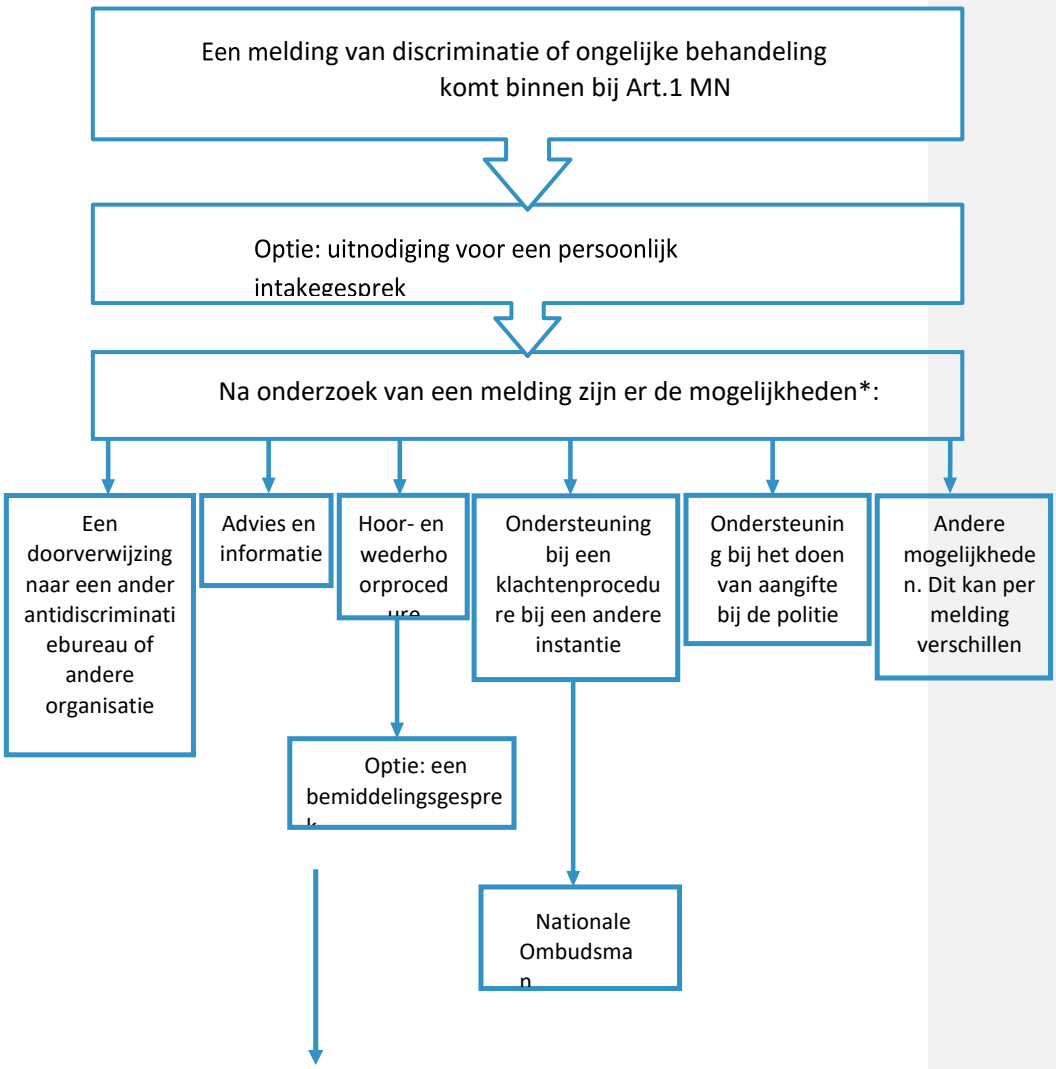
1.1 Ingevolge artikel 37, eerste lid, onderdeel c, van de AVG is Tûmba verplicht een functionaris gegevensbescherming (hierna: FG) aan te stellen. Tûmba heeft te allen tijde minimaal één FG in dienst voor de handhaving en naleving van de AVG bij Tûmba;
1.2 De FG is de contactpersoon tussen Tûmba en de Autoriteiten Persoonsgegevens;
1.3 De FG wordt door de directeur van Tûmba gekozen;
1.4 Voor het aanstellen van een FG wordt online het aanmeldingsformulier functionaris gegevensbescherming ingevuld[5].

[5] Formulier FG: https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/aanmelding_fg.pdf

BIJLAGE 1

Protocol Behandeling meldingen Tumba: Zie onderstaande link

https://beeldschrift.nl/CMS/api/file/tumba/461aaab800e1111fd1799ce01aba0445/



STAPPENPLAN VOOR DE BEHANDELING VAN EEN MELDING

Met opmerkingen [AS10]: aangepast stroomdiagram voor Tûmba maken

*Tûmba kan te allen tijde besluiten een melding te sluiten.

BIJLAGE 2

Machtigingsformulier klachtbehandeling en informatie opvragen bij/verstrekken aan derden

Hierbij verleen ik, ……, toestemming aan Tûmba (het Discriminatie Meldpunt Friesland), gevestigd aan het Stationskwartier, Snekertrekweg 1, 8912 AA te Leeuwarden, om (bijzondere) persoonsgegevens te registreren, te verstrekken aan derden en/of op te vragen bij derden. Dit doen we altijd in overleg met u. Wij verwerken uw persoonsgegevens om u te

Het College voor de Rechten van de Mens

ondersteunen en uw klacht te behandelen.

Datum : ……

Plaats : ……

Handtekening cliënt : ……

BIJLAGE 3

Protocol Databeveiliging

Deel I. Papieren dossiers

1. Alleen medewerkers en stagiairs van de afdeling Klachtbehandeling hebben toegang tot de papieren dossiers.
2. Tûmba heeft alleen gesloten dossiers op papier. De papieren dossiers vormen dus een archief. Er wordt *niet* gestreefd naar nieuwe lopende papieren dossiervorming.
3. De papieren dossiers worden opgeborgen in afgesloten kasten tenzij medewerkers er direct mee aan het werk zijn. De sleutels van de kasten worden opgeborgen op de door de afdeling Klachtbehandeling gekozen plaatsen.
4. Papieren dossiers, of onderdelen daarvan, mogen alleen buiten kantoor worden gebracht in een ondoorzichtige tas.
5. Voordat een dossier meegenomen wordt naar huis of locatie, worden het nummer van het dossier, de locatie, de initialen van de medewerker, en de data waarop het wordt meegenomen en is teruggebracht in een bestand geregistreerd. De registratie wordt gecontroleerd door een aangewezen persoon van de afdeling Klachtbehandeling, die dit bespreekt in het klachtoverleg.
6. Voordat een dossier wordt meegenomen wordt een volledige gescande kopie van het dossier opgeslagen of een fysieke kopie achtergelaten in een afgesloten kast.

Met opmerkingen [AS11]: ACTIE: aanmaken digitaal bestand (excel) over papieren dossiers

Deel II. Digitaal registratiesysteem

1. Tûmba maakt *uitsluitend* gebruik van ADV-net voor het registreren van de meldingen;

2. Verschillende medewerkers van het meldpunt hebben toegang tot verschillende onderdelen van het digitale registratiesysteem, al naar gelang deze toegang nodig is voor het verwezenlijken van de doeleinden van de organisatie;

3. Inloggegevens van het digitale registratiesysteem worden geheimgehouden, de browser wordt ingesteld om de inloggegevens niet te onthouden;

4. De beveiliging en validiteit van ADV-net is landelijk geregeld door de LVtD.

Met opmerkingen [AS12]: Wie beheert ADV-net? Is dit inderdaad LVtD?

Met opmerkingen [JZ13R12]: dit klopt inderdaad. Uitgezocht.

Deel III. Bestandsbeheer en dataopslag op kantoor

1. Bestanden en data die betrekking hebben op meldingen en klachten (mails, fysieke en digitale aantekeningen, documenten) worden opgeslagen in ADV-net. Deze gegevens mogen niet worden opgeslagen op de netwerkschijven van de laptops;

2. De medewerkers van het meldpunt controleren dagelijks of er geen bestanden met persoonsgegevens zijn achtergebleven op de laptops.

3. Inloggegevens op het serversysteem worden geheimgehouden, de browser wordt ingesteld om de inloggegevens niet te onthouden.

Met opmerkingen [AS14]: Hoe dan? Astrid

Met opmerkingen [JZ15R14]: 29 juni Harry gemaild met vraag of hij weet hoe dit moet

Met opmerkingen [AS16R14]: Harry weet inderdaad hoe dit moet. Hij maakt een ronde langs alle collega's om te bespreken hoe ze hun browser zó kunnen instellen dat er geen gegevens worden onthouden / automatisch worden ingevuld.

4. Gasten mogen niet op de inlognaam van medewerkers gebruik maken van de computers.

5. Indien een medewerker of stagiair vertrekt, wordt op de dag van de beëindiging van zijn arbeids- of stageovereenkomst ook zijn bevoegdheid tot bereiken van de papieren en digitale dossiers alsmede van zijn account stopgezet.

Deel IV. Draagbare apparaten

1. Laptops en digitale bestandsdragers die buiten kantoor worden gebracht zijn beveiligd met een wachtwoord;

2. Op laptops, telefoons of andere apparatuur die buiten kantoor worden gebracht zijn geen inloggegevens opgeslagen van medewerkers;

3. Het digitale registratiesysteem is niet meteen toegankelijk bij toegang tot de draagbare apparatuur van medewerkers en de inloggegevens zijn niet opgeslagen op de draagbare apparatuur;

4. Het besturingssysteem wordt dusdanig ingesteld dat er geen gegevens automatisch worden ingevuld. De FG-er ziet erop toe dat de medewerkers hun instellingen *up to date* hebben.

BIJLAGE 4

Protocol Datalekken

Deel I. Algemene artikelen

1. Er is sprake van een *datalek* bij onbedoelde of onwettige vernietiging, verlies, wijziging of ongeautoriseerde toegang (door onbevoegden) tot de gegevens van melders;
2. Het datalek wordt gemeld als niet uit te sluiten is dat het verlies of onrechtmatige verwerking *leidt tot de aanzienlijke kans op ernstige nadelige gevolgen dan wel ernstige nadelige gevolgen heeft voor de bescherming van persoonsgegevens.* Indien het vernietigde, verloren, gewijzigde of bekeken materiaal door onbevoegden geen informatie bevat wat te herleiden is naar de melder(s), spreken we niet van een datalek;
3. Bij het vaststellen van een lek wordt eerst zo snel en goed mogelijk onderzocht wat de grootte is van het lek. In geval van een lek in het digitale registratiesysteem en op de laptops moet hiervoor hulp gevraagd worden van IT-specialisten en de systeembeheerder. Bij papierendossiers moet geteld worden om hoeveel dossiers het gaat;
4. Hierna wordt zo snel mogelijk onderzocht wie betrokken zijn bij het lek en hoe lang het lek al bestaat.

Deel II. Informatieverstrekking binnen de organisatie

1. Bij enig lek wordt, na dat het onderzoek in deel I is afgerond, als eerste contact opgenomen met de verantwoordelijke/de directeur om hen in te lichten over de grootte, de aard, en de verantwoordelijke voor het lek.
2. Bij afwezigheid van de directeur wordt contact opgenomen met de voorzitter van het bestuur.

Deel III. Elektronische lekken

1. Bij een lek in het digitale registratiesysteem wordt zo snel mogelijk contact opgenomen met de makers van het digitale registratiesysteem om te bekijken hoe groot het lek is, waar het door komt, wat er gebeurd is en welke gegevens hoe lang zijn bekeken of verwerkt.
2. Bij een lek in het serversysteem wordt zo snel mogelijk door de systeembeheerder onderzocht hoe groot het lek is, wat de oorzaak is, wie de slachtoffers zijn en welke gegevens hoe lang zijn bekeken of verwerkt.

Deel IV. Maatregelen om het lek te dichten

1. Er wordt zodra er bekend is wat de aard van het lek is actie ondernomen om het lek te dichten.

2. Bij een lek in het digitale registratiesysteem wordt zo snel mogelijk contact opgenomen met de makers van het digitale registratiesysteem om het lek te dichten.
3. Bij een lek in het serversysteem wordt zo snel mogelijk contact opgenomen met de systeembeheerder om het lek te dichten. De beheerder ontvangt tevens per direct een melding als er een (vermoeden van een) lek plaatsvindt op het systeemserver.
4. Bij een lek in de papierendossiers wordt eerst geprobeerd de dossiers zelf te redden of terug te halen indien mogelijk. Als dit niet mogelijk is, wordt zo snel mogelijk de politie of andere relevante handhavingsinstantie ingeschakeld om de dossiers terug te vinden of te redden.

Deel V. Melding bij de Autoriteit Persoonsgegevens

1. Na vaststelling van het bestaan van het lek wordt door degenen genoemd in Deel II uiterlijk binnen 72 uur nadat er kennis is genomen van het lek een melding gemaakt bij de Autoriteit Persoonsgegevens (artikel 33, eerste lid, van de AVG).
2. Bij de melding wordt gemeld aan de hand van het formulier in de bijlage, gebaseerd op het richtsnoer van de Autoriteit Persoonsgegevens (bijlage 1). Zoveel mogelijk informatie wordt gemeld.
3. Indien er informatie die gemeld moet worden later bekend wordt dan het tijdstip van de melding, wordt deze door degenen genoemd in Deel II aangevuld.

Deel VI. Informatieverstrekking aan de betrokkenen

1. Na vaststelling van het lek wordt door degenen genoemd in Deel II contact opgenomen met de getroffenen. Dit gebeurt zodra er in elk geval bekend is wat de aard van het lek is, zoals beschreven in Deel I, art. 3 en 4, en Deel III.
2. Aan de betrokkenen wordt gemeld:
   - wat de aard is van het datalek
   - om welke gegevens het gaat
   - welke mogelijke partijen toegang hebben tot de gegevens
   - wat de mogelijke gevolgen zijn van het datalek
   - welke maatregelen zijn/worden genomen om het lek te dichten
   - welke maatregelen zijn/worden genomen om herhaling te voorkomen.

Deel VII. Informatieverstrekking aan de buitenwereld.

1. Is informatie over het lek in de media terechtgekomen, dan komen directeur, de communicatiemedewerker en degene(n) die het lek hebben veroorzaakt/ontdekt zo snel mogelijk bij elkaar. Na het volgen van de rest van de procedure (Deel I-IV), stellen

zij een persbericht op dat naar de media verzonden kan worden. De directeur brengt het bestuur op de hoogte. De directeur bepaalt of het bericht naar de media kan. De daaropvolgende contacten met de media zijn

2. Bij een datalek met een grootte vanaf 100 getroffenen, of een datalek waarvan het aantal getroffenen onbekend is, komen directeur, communicatiemedewerker en degene die het lek heeft veroorzaakt/ontdekt zo snel mogelijk bij elkaar. Na het volgen van de rest van de procedure, stellen zij een persbericht op en bepalen op welke manier en naar wie dit verspreid moet worden. De directeur brengt het bestuur op de hoogte. De directeur bepaalt of het bericht naar de media kan. De daaropvolgende contacten met de media zijn of met de directeur of met de communicatiemedewerker.