Ministerie van Justitie en Veiligheid

Handelingskader doxing

Handvatten voor werkgevers om de impact op medewerkers te verminderen

Colofon

Opdrachtgever
Werkgroep Veilig werkgeverschap van de Taskforce
Onze Hulpverleners Veilig | Ministerie van Justitie en Veiligheid

Verantwoordelijk uitvoerende
ARQ Nationaal Psychotrauma Centrum |
ARQ Kenniscentrum Impact van Rampen en Crises

Nienoord 5
1112 XE Diemen
info@arq.org
www.arq.org

Auteurs
Dr. Fieke Bruggeman-Everts
Wera van Hoof, MSc
Dr. Hans te Brake

Jaar van uitgave
2023

Inhoudsopgave

Samenvatting

Dit handelingskader biedt werkgevers handvatten voor het omgaan met doxing. Met als doel om de impact van doxing op medewerkers met een publieke taak te verminderen. Ook kunnen leidinggevenden en medewerkers kennis ontlenen aan dit handelingskader.

Doxing wordt ook wel omschreven als intimidatie met persoonsgegevens. Dit handelingskader beschrijft drie fases bij doxing: ‘preventie’, ‘handelen bij doxing’ en ‘nazorg’.

Bij preventie van doxing is het belangrijk dat je als werkgever zorgt dat medewerkers en leidinggevenden weten wat doxing is en dat zij vaardigheden ontwikkelen om met doxing om te gaan. Daarnaast moet er ondersteuning zijn en duidelijkheid over wie waarvoor verantwoordelijk is binnen de organisatie zodra er sprake is van doxing.

Bij (een vermoeden van) doxing is het belangrijk dat daar melding van wordt gedaan bij de organisatie. Ook is het van belang dat er een persoonlijk aanspreekpunt is voor de medewerker, zodat alles in afstemming met de medewerker (en diens naasten) gebeurt. Het is de taak van de werkgever om te ondersteunen bij het doen van melding of aangifte van doxing bij de politie. Ook is het aan de werkgever om, wanneer nodig, beveiliging en psychosociale ondersteuning te regelen.

Is het incident is afgehandeld en de mate van bedreiging gezakt? Dan is het belangrijk dat je als werkgever steun blijft bieden en dat er lessen worden getrokken uit het incident.

Inleiding

Wat is doxing?

Doxing is het (digitaal) aanbieden of verspreiden van identificerende persoonsgegevens, met de intentie om vrees aan te (laten) jagen, ernstige overlast aan te (laten) doen of de medewerker in zijn ambt of beroep ernstig te (laten) hinderen. Anders gezegd: om anderen lastig te vallen of te intimideren. Denk aan persoonsgegevens als een naam, adres of beeldmateriaal. Steeds vaker krijgen medewerkers met een publieke taak (vanaf nu 'medewerkers') te maken met doxing.

Sinds 1 januari 2024 is het verschaffen, verspreiden of op een andere manier ter beschikking stellen van persoonsgegevens voor intimiderende doeleinden strafbaar (zie Wet strafbaarstelling gebruik persoonsgegevens voor intimiderende doeleinden). Doxing is nu een strafbaar feit waarvoor je aangifte kunt doen. Doxing gaat vaak samen met ander strafbaar gedrag richting medewerkers. Zoals bedreiging, intimidatie, belediging, opruiing, stalking en/of hinderen in het werk. Naast aangifte tegen doxing, kun je apart aangifte doen voor bijvoorbeeld intimidatie of ander strafbaar gedrag na doxing. Dit handelingskader gaat alleen over doxing.

Wat is de impact van doxing?

Doxing is een vorm van agressie die vaak de privésituatie van de medewerker raakt. Het is anders dan alleen fysieke of verbale agressie op straat. Je persoonlijke situatie (je eigen huis of dat van je naasten) wordt vaak snel en fors bedreigd. Het is vaak onduidelijk hoe hevig de gevolgen van doxing zijn. De gevolgen kunnen ook permanent zijn: je weet vaak niet hoe lang de dreiging blijft of wanneer het weer oplaait. Die angst kan impact hebben op het welzijn, de privésituatie, de sociale omgeving en de taakuitoefening van de medewerker.

Over dit handelingskader

Doel van het handelingskader

Volgens de Arbeidsomstandighedenwet (Arbowet) moet de werkgever beleid voeren gericht op het voorkomen of beperken van psychosociale arbeidsbelasting als dit een risico is binnen de organisatie. Doxing is hier een voorbeeld van. Dit handelingskader biedt werkgevers handvatten voor het omgaan met doxing. Het bevat aanbevelingen over psychosociale en praktische ondersteuning bij doxing. Het handelingskader draagt bij aan het verminderen van de negatieve impact van doxing op de medewerker. Ook kunnen leidinggevenden en medewerkers kennis ontlenen aan dit handelingskader.

Toepassing van het handelingskader

Dit handelingskader beschrijft drie fases bij doxing: 'preventie', 'handelen bij doxing' en 'nazorg'. Bij elke fase worden belangrijke onderwerpen genoemd om in overweging te nemen. Waar mogelijk worden praktische aanbevelingen gegeven.

Het is de bedoeling dat iedere werkgever van medewerkers met een publieke taak dit generieke handelingskader kan vertalen en integreren in bestaande werkprocessen en kwaliteitsdoelstellingen. Ook kunnen werkgevers zelf invulling geven aan de aanbevelingen in dit handelingskader. Dit is afhankelijk van de eigen professionele verantwoordelijkheid, mogelijkheden en werkwijzen binnen de verschillende organisaties.

Totstandkoming

De aanbevelingen in dit handelingskader zijn met zorg samengesteld op basis van een verkennende studie naar relevante (wetenschappelijke) literatuur, rapporten en websites (zie bronvermelding onderaan het handelingskader). Dit is aangevuld met kennis uit de praktijk die verzameld is onder vertegenwoordigers van de politie, brandweer en boa's. Hierbij is ook een ervaringsdeskundige betrokken. De werkgroep Veilig werkgeverschap van de Taskforce Onze Hulpverleners Veilig en diverse experts (VPT-coördinatoren, Arbospecialisten en juridisch adviseurs) zijn betrokken in de commentaarfase.

Handelingskader doxing

Handvatten voor werkgevers om de impact op medewerkers te verminderen

Preventie

Het is van belang dat medewerkers en leidinggevenden weten wat doxing inhoudt en hoe ze ermee omgaan, en dat ze hier de vaardigheden ook voor hebben. Daarnaast moet er ondersteuning en duidelijkheid zijn over wie waarvoor verantwoordelijk is binnen de organisatie zodra er sprake is van doxing.

Zorg voor kennis en vaardigheden op het gebied van doxing

1. Zorg voor trainingen en informatievoorziening waarin de volgende aspecten aan bod komen:
   - Maak medewerkers en leidinggevenden bewust van het fenomeen doxing, zodat ze het herkennen. Bespreek bijvoorbeeld met elkaar: Wat is doxing? En wat niet? Wat is strafbaar en wat niet? Hoe herken je het en wat moet je doen als het jou of een collega overkomt? Wat voor impact kan het hebben op jou en je werk?
   - Geef medewerkers voorlichting over veilig gebruik van sociale media en internet. Daaronder valt het afschermen van digitale persoonsgegevens en goede cyberveiligheid. Ook voor de naasten van de medewerker is die informatie van belang.
   - Train medewerkers in het omgaan met gefotografeerd of gefilmd worden tijdens het werk. Medewerkers worden regelmatig gefilmd tijdens het werk, en de filmer kan daar verschillende redenen voor hebben. Maak medewerkers ervan bewust dat het strafbaar is als het doel ervan is om hen lastig te vallen of te intimideren. Zorg ervoor dat medewerkers verschillende casussen met elkaar bespreken, zodat zij adequaat kunnen handelen tijdens het werk.
   - Communiceer naar zowel medewerkers als burgers dat elke vorm van agressie en intimidatie richting medewerkers onacceptabel is.
   - Leg zowel medewerkers als burgers uit wat de doxingwet voor iedereen betekent. Leg ook uit welke risico's er zijn als je andermans persoonsgegevens deelt: een ander kan deze gegevens gebruiken om te doxen.
2. Bespreek het risico op doxing in briefings voordat medewerkers worden ingezet. Bekijk per situatie of er een kans is op doxing, en hoe in dat geval het beste gehandeld wordt. Hierbij kan een deskundige op het gebied van maatschappelijke onrust of communicatie ondersteunen. Dit wordt mogelijk belegd bij een centraal informatiepunt, zie punt 8.
3. Wees ervan bewust dat beeldmateriaal iemand kwetsbaar kan maken voor doxing. Het gaat hier om beeldmateriaal dat tot de persoon te herleiden is, bijvoorbeeld een webpagina met foto's van alle medewerkers, een intern 'smoelenboek' of externe communicatiemiddelen.
4. Zorg voor een mogelijkheid om het werk na te bespreken. Doe dat in een open, veilige en lerende sfeer. Zo kunnen medewerkers met elkaar de signalen van doxing (en mogelijke impact op de medewerkers) herkennen. Bespreek het omgaan met normoverschrijvend gedrag op het werk, zodat medewerkers leren waar de grens ligt. Denk daarbij ook aan bedreiging, intimidatie, belediging, opruiing, stalking en/of hinderen in het werk. Bespreek bovendien dat een gevoel van intimidatie of beperkt worden in de taakuitoefening al voldoende reden is om de situatie te bespreken met de leidinggevende of collega's.

Zorg dat de organisatie is voorbereid op een doxingincident

5. Zorg dat opvang en nazorg is geregeld, conform de Richtlijn Psychosociale Ondersteuning Geüniformeerden. Zorg dat medewerkers en leidinggevenden weten waar ze (een vermoeden van) doxing kunnen melden binnen de organisatie waar ze werken. Regel vooraf al de mogelijkheid om collegiale ondersteuning in te zetten en maak duidelijk hoe en waar medewerkers dit kunnen krijgen. Regel, conform de Arbowet, dat medewerkers professionele hulpverlening kunnen krijgen zodra ernstige klachten worden geconstateerd. De leidinggevende, coördinator of opleider kan getraind worden in het aansturen van collegiale ondersteuning.
6. Verken de mogelijkheden om als werkgever onrechtmatige of strafbare content te achterhalen en te laten verwijderen op internetplatforms. Zo ben je als werkgever bekend met deze procedures. Het kan helpen om deskundigen te betrekken op het gebied van sociale media en Open Source Intelligence (OSINT). Bekijk voor meer informatie over het achterhalen en laten verwijderen van content: de Notice-and-Takedownprocedure (NTD-procedure), Digital Service Act (DSA-verordening) en Project Online Content Moderatie (PrOCoM). Zie de begrippenlijst onderaan het handelingskader.

Beleg verantwoordelijkheden

7. Beleg preventie, melding, afhandeling, opvang en nazorg rondom doxing bij een partij en/of een persoon binnen de organisatie. Daar komt dan (ervarings)kennis samen en hier kunnen medewerkers naartoe voor vragen en ondersteuning. Dit is in overeenstemming met de Arbowet.
8. Bundel kennis en ervaring rondom doxing landelijk en maak dit beschikbaar via een (landelijk) centraal informatiepunt. Is er vermoeden van doxing, dan kan deze informatievoorziening geraadpleegd worden. Daarnaast kan algemene kennis en ervaring uit verschillende organisaties via dit informatiepunt worden gebundeld. Zo kunnen algemene adviezen worden geëvalueerd.

Handelen bij een incident

Bij (een vermoeden van) doxing is het belangrijk dat daar melding van wordt gedaan bij de organisatie. Zo kunnen de juiste stappen worden genomen. Bied zowel praktische als psychosociale ondersteuning als er sprake is van doxing en heb oog voor de persoonlijke situatie van de medewerker.

Meld het incident

9. Zodra er sprake (of een vermoeden) is van doxing, moet het incident direct gemeld worden bij het aanspreekpunt in de organisatie. Bijvoorbeeld de leidinggevende. Van elk normoverschrijdend gedrag tegen een medewerker moet een melding gemaakt worden, ongeacht of er sprake is van een strafbaar incident. Denk ook aan gedragingen als bedreiging, intimidatie, belediging, opruiing, stalking en/of hinderen in het werk. Meld alle (vermoedens van) incidenten in een eigen registratiesysteem (conform de Wet algemene verordening gegevensbescherming). Zo ontstaat er een compleet beeld van alle incidenten. Zorg dat het doen van een melding zo laagdrempelig mogelijk is.
10. Verzamel zo veel mogelijk bewijsmateriaal van het incident. Zorg dat de datum, tijd en URL zichtbaar zijn op screenshots.
11. Bij voorkeur is er één aanspreekpunt in de organisatie voor het melden van doxingincidenten. Deze persoon coördineert vanaf het begin de inzet of betrokkenheid van alle verschillende afdelingen. Ook voorziet diegene zo veel mogelijk in maatwerk voor ondersteuning aan de betrokken medewerker(s).
12. Schat in of het uitnodigen van de mogelijke dader(s) voor een informerend gesprek, kan bijdragen aan het proces of zelfs aan het stoppen van het wangedrag. Stem dit af met de medewerker en bekijk nauwkeurig per casus of het voeren van een dergelijk gesprek een verstandige keuze is. Zo'n gesprek sluit andere acties niet uit, zoals melding of aangifte doen bij politie.
13. Vermoed je strafbare doxing, stem de eventuele acties richting de mogelijke dader(s) af met de politie.
14. Stem eventueel optreden of acties in de media eerst intern af, binnen de organisatie en met de gedoxte medewerker en diens naasten. Bespreek wat een behulpzame communicatiestrategie kan zijn en schakel deskundigheid op het gebied van communicatie in. Soms is assertief stelling nemen over het incident behulpzaam. Andere keren is stilhouden een betere aanpak om een mediastorm te voorkomen.

Bied psychosociale ondersteuning aan

15. Ieder doxingincident is verschillend qua context, verloop en gevolgen. De precieze manier van handelen vereist dus maatwerk. De gedoxte medewerker staat echter altijd centraal. Zorg dat de leidinggevende of teamleider regelmatig informeert hoe het gaat en vraagt naar behoeften van de medewerker en diens naasten. Ook tijdens bijvoorbeeld een beveiligingsperiode. Informeer of naasten van de medewerker, zoals familie, vrienden en collega's (mogelijk met eenzelfde ervaring), steun kunnen bieden. Bespreek het incident ook met het team en informeer hoe het met het team gaat. De leidinggevende of teamleider moet tijd vrij kunnen maken in de agenda om deze informerende rol uit te voeren.
16. Betrek de medewerker bij besluitvorming. Praat mét en niet over de persoon.
17. Bied ongeveer 24 tot 48 uur na het doxingincident proactief collegiale ondersteuning aan. Houd je aan de principes van 'watchful waiting'. Dit betekent dat het enerzijds belangrijk is om niet te afwachtend te zijn en problemen over het hoofd te zien, anderzijds is het zaak om geen onnodige of verkeerde hulp te bieden of op te dringen. Worden er ernstige klachten geconstateerd, dan zorg je voor laagdrempelige doorverwijzing naar professionele zorg door specialisten. Zie de Richtlijn Psychosociale Ondersteuning Geüniformeerden voor meer informatie over opvang en nazorg bij ingrijpende gebeurtenissen op het werk.
18. Heb als werkgever ook oog voor het welzijn van de betrokken collega's en de leidinggevende(n) of teamchef van de medewerker. Ook zij moeten ondersteund worden in het bieden van ondersteuning aan de medewerker. Houd regelmatig intervisie en monitor regelmatig hoe het gaat.

Bied praktische ondersteuning aan

19. Ondersteun de medewerker bij het doen van melding of aangifte van het incident bij de politie. Je kunt als werkgever melding of aangifte doen en de medewerker als getuige laten optreden, maar de medewerker kan ook zelf melding of aangifte doen. Zie de Werkinstructie werkgever en werknemer bij aangifte/melding en de Factsheet anoniem aangifte doen voor meer informatie. Er moet aangegeven worden dat het om een VPT-zaak (Veilig Publieke Taak) gaat, zodat de aangifte prioriteit krijgt. Soms wil een medewerker om bepaalde redenen geen melding of aangifte doen. Vraag hiernaar en begeleid de medewerker zorgvuldig, zodat de medewerker zelf ook een actieve rol kan innemen in het proces. Als de medewerker (naar aanleiding van doxing) te maken krijgt met intimidatie of andere vormen van agressie en geweld, dan kan daar uiteraard ook apart melding of aangifte van gedaan worden.
20. Betrek een specialist bij het achterhalen en beoordelen van onrechtmatige of strafbare online content, en bij het verzoeken om content te laten verwijderen van internetplatforms. Zorg voor een scan van sociale media (zie ook punt 6 van dit handelingskader). Laat dit bij voorkeur niet doen door de medewerker zelf of door collega's, omdat dit belastend kan zijn. Dit kan namelijk grote impact hebben en uitnodigen tot inmenging in de berichtgeving op sociale media. Alleen in uitzonderlijke gevallen kan de medewerker zelf de berichtgeving volgen en bewijsmateriaal verzamelen.

Zorg voor persoonlijke beveiliging indien nodig en houd rekening met de impact van bewaakt en beveiligd worden

21. Beleg de beveiliging van de medewerker (en mogelijk diens naasten) bij een afdeling of persoon binnen de organisatie die een inschatting kan maken van de ernst van de situatie. Je bent als werkgever primair verantwoordelijk voor het omgaan met de dreiging. Indien nodig kun je deskundigheid inwinnen bij de politie. Zorg dat de maatregelen omtrent bewaken en beveiligen worden georganiseerd met inspraak van de medewerker en diens naasten. Bespreek na verloop van tijd met de beveiligende partij en de medewerker of de maatregelen nog nodig zijn. Begeleid de medewerker ook als de maatregelen worden afgebouwd.
22. Wees ervan bewust dat de maatregelen omtrent bewaking en beveiliging ook veel impact hebben op de medewerker en diens privéomgeving. Laat maatregelen daarom aansluiten op de persoonlijke omstandigheden en behoeften van de medewerker en diens naasten.

Nazorg

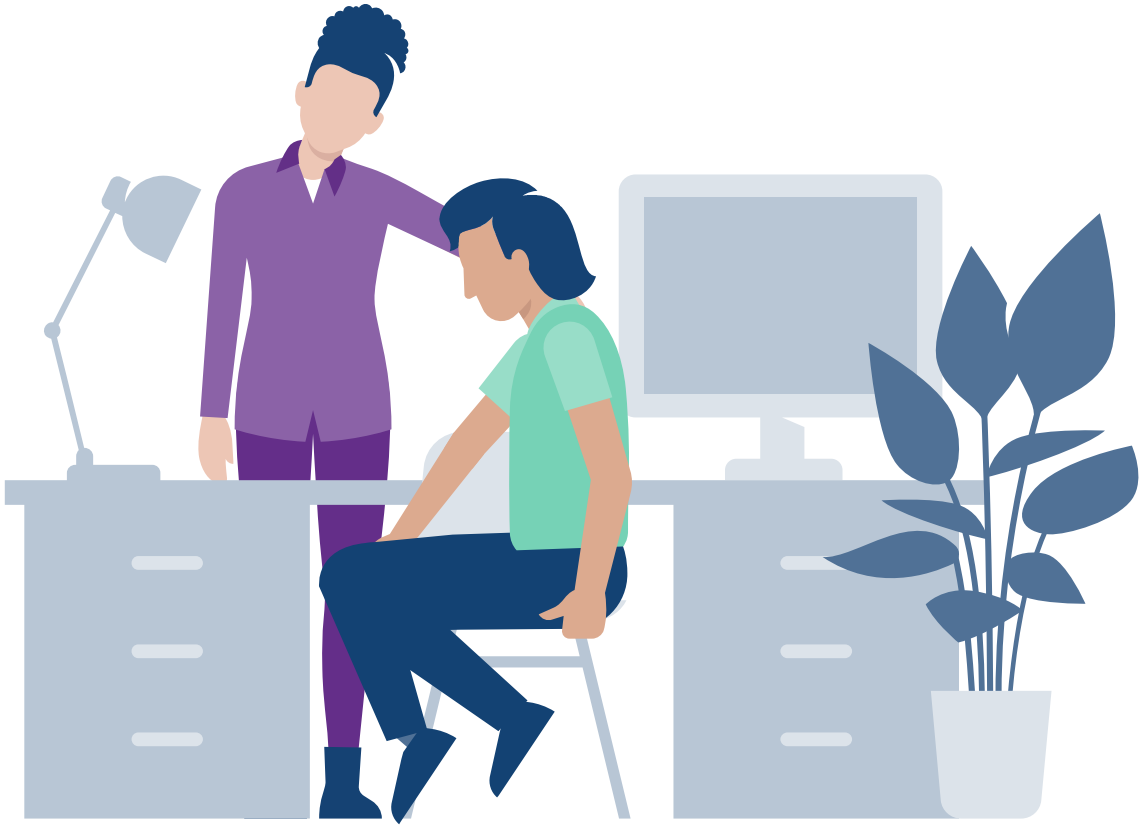
Is het incident afgehandeld en de mate van bedreiging gezakt, blijf dan nog steeds steun bieden en evalueer het incident.

Blijf steun bieden aan de medewerker en naasten, ook op de lange termijn

23. Licht de medewerker en naasten in over momenten in de toekomst waarop de bedreiging weer kan oplaaien. Zoals media-aandacht voor het incident, eindejaarsoverzichten, herdenkingsbijeenkomsten, politieke debatten, een hoorzitting of een rechtszaak.
24. Ga bij de medewerker na hoe het incident het werk beïnvloedt. Het incident kan een langdurig onveiligheidsgevoel geven. Blijf in gesprek met de medewerker, maar ook met het team. Vraag hoe de medewerker kan terugkeren naar een gewenste situatie en wat diegene daarvoor nodig heeft. Inventariseer wie daarbij gepaste hulp kan bieden, zoals familie, naasten, collega's en professionele hulpverleners.
25. Blijf een specialist betrekken bij mogelijke oplaaimomenten. Die kan het in de gaten houden en online berichtgeving verzamelen. Laat deze specialist online persoonsgegevens en restanten van de mediastorm verwijderen.

Evalueer het incident

26. Bespreek met de medewerker en het team wat zij kunnen leren van het incident.
27. Breng de expertise die medewerkers hebben opgedaan bij doxingincidenten samen in de organisatie. Breng deze informatie ook samen in bijvoorbeeld een landelijk informatiepunt. Zo worden algemene kennis en ervaring uit verschillende organisaties gebundeld en kunnen algemene adviezen geëvalueerd worden (zie ook punt 8 van dit handelingskader).
28. Waarborg de privacy van de medewerker bij de evaluatie.



Bronvermelding

- Website Veilig Publieke Dienstverlening, via https://www.veiligepubliekedienstverlening.nl
  - Factsheet over anonimiteit in het strafproces
  - Werkinstructie werkgever en werknemer bij aangifte/melding
- Eerste hulp bij Online Haat van DeGoedeZaak, via https://eerstehulpbijonlinehaat.nl/
- Zelfscan CCV, via https://hetccv.nl/themas/integraal-veiligheidsbeleid/veiligheid-politieke-ambtsdragers/
- Website Weerbaar Bestuur, via https://www.weerbaarbestuur.nl/
  - Eerste hulp bij intimidatie social media
  - Agressieprotocol voor politieke ambtsdragers:
  - Zorg voor politieke ambtsdragers
- Website Weerbare Overheid, via https://weerbareoverheid.nl/
- Website Autoriteit persoonsgegevens, via https://www.autoriteitpersoonsgegevens.nl/
  - Privacy rechten AVG
- VSNU (2021). Handreiking Aanpak bedreiging wetenschappers. Verkregen op 13-12-2023 via https://www.ru.nl/sites/default/files/2022-11/vsnu_handreiking_aanpak_bedreiging_wetenschappers.pdf
- Rathenau Instituut (2021). Online ontspoord – Een verkenning van schadelijk en immoreel gedrag op het internet in Nederland. Den Haag. Verkregen op 13-12-2023 via https://www.rathenau.nl/nl/digitalisering/online-ontspoord
- N. Ree (2021). Politie als prooi - Een verkennend onderzoek naar de vraag hoe Nederlandse politieagenten het slachtofferschap van doxing ervaren. Masterscriptie Bestuurskunde – Besturen van veiligheid; Faculteit der Sociale Wetenschappen, Vrije Universiteit te Amsterdam.
- J. van Heerikhuizen (2023). When the shit hits the fan- Een verkennend onderzoek naar de ervaren collegiale opvang en ondersteuning van gedoxte Nederlandse politieagenten. Masterscriptie Politieacademie; Apeldoorn. Verkregen op 13-12-2023 via https://www.politieacademie.nl/kennisenonderzoek/kennis/mediatheek/PDF/103064.PDF
- FERRO (2021). Sociale norm agressie en geweld richting hulpverleners. Verkregen op 13-12-2023 via https://open.overheid.nl/documenten/ronl-e92d21c3-95b6-45dc-91ba-3291e5df4607/pdf
- ARQ (2012). Richtlijn psychosociale ondersteuning geüniformeerden. Verkregen op 13-12-2023 via https://arq.org/diensten/richtlijn-psychosociale-ondersteuning-geuniformeerden
- ARQ (2020). Onderzoeksrapport Psychosociale effecten van bedreiging en beveiliging. Verkregen op 13-12-2023 via https://arq.org/publicaties/psychosociale-effecten-van-bedreiging-en-beveiliging
- ARQ (2022). Onderzoek psychosociale gevolgen van dreiging en beveiliging bij advocaten en rechters. Verkregen op 13-12-2023 via https://www.rijksoverheid.nl/documenten/rapporten/2023/01/27/tk-bijlage-onderzoeksrapportage-psychosociale-gevolgen-van-dreiging-en-beveiliging-bij-advocaten-en-rechters
- ARQ (2016). Getagd voor het leven - Een verkennende studie naar de effecten op professionals van het filmen en online plaatsen van (beeld)materiaal van professioneel handelen. Verkregen op 13-12-2023 via https://arq.org/publicaties/getagd-voor-het-leven
- Actieprogramma Taskforce Onze hulpverleners veilig. Verkregen op 13-12-2023 via https://www.rijksoverheid.nl/documenten/publicaties/2021/03/29/actieprogramma-taskforce-onze-hulpverleners-veilig
- Wetsvoorstel Strafbaarstelling gebruik persoonsgegevens voor intimiderende doeleinden en Memorie van toelichting 2021 – 2022 van De Minister van Justitie en Veiligheid, D. Yesilgöz-Zegerius
- Wet strafbaarstelling gebruik persoonsgegevens voor intimiderende doeleinden (Stb. 2023, 274)
- Vrijheid van informatiegaring: https://www.anp.nl/blog/305/privacywetgeving-mag-je-filmen-op-de-openbare-weg
- Portretrecht: https://www.anp.nl/blog/201/anp-portretrecht

Begrippenlijst

DSA. De Digital Services Act (DSA) vormt de toekomstige basis voor digitale diensten zoals online platforms en verduidelijkt hun verantwoordelijkheden op het gebied van hun werkzaamheden.

Landelijk informatiepunt voor doxing. Op het moment van de uitgave van dit handelingskader, was er nog geen sprake van een dergelijk informatiepunt. Bij een landelijk informatiepunt moet ten minste de volgende informatie of verwijzing naar specialisten te vinden zijn:

- Informatie over motieven om te doxen, zodat je kans op doxing beter kunt inschatten in de preparatiefase
- Informatie over een communicatiestrategie voor gebruik van (sociale) media bij een incident
- Deskundigheid over veiligheidsdreiging
- Eventueel een opleidingsmodule over doxing voor coördinatoren in de organisaties

NTD. Met de Notice-and-takedownprocedure (NTD) kun je een verzoek indienen op het moment dat je informatie tegenkomt waarvan je denkt dat deze onrechtmatig of strafbaar is. Als de provider of eigenaar van de website waar deze content staat de melding ontvangt, moet deze de content verwijderen of de toegang ertoe blokkeren, tenzij deze aantoont dat de content legitiem is.

OSINT. Open source intelligence (OSINT)-specialisten van de politie speuren zowel publiek toegankelijke (internet)bronnen als minder toegankelijke (internet)bronnen zoals het Deepweb en Darkweb af naar informatie die de bewijslast voor onderzoeken verzwaart.

PrOCoM. Het Project Online Content Moderatie (PrOCoM) biedt een publiek-privaat kader waarbinnen burgers, overheid en de internetsector makkelijker kunnen handelen bij online materiaal dat strafbaar is, schade toebrengt of maatschappelijk ongewenste effecten met zich meebrengt. Zie ook informatie over Integraal veiligheidsbeleid op de website van Centrum voor Criminaliteitspreventie en Veiligheid (CCV) via www.hetccv.nl.

Wat kan je zelf doen bij doxing?

Handvatten bij intimidatie met persoonsgegevens

Wees voorbereid

Wees je bewust

Wat is doxing en wat niet? Hoe herken je het? Bespreek dit met je collega's en lees je in.

Waar melden

Zorg dat je weet hoe en bij wie je doxing kan melden op je werk.

Stel grenzen

Praat op het werk over gedrag dat jullie niet oké vinden. Waar ligt de grens?

Internetveiligheid

Check regelmatig hoe vindbaar je bent online. Vind je ergens je persoonsgegevens? Stuur een e-mail of brief aan de organisatie om deze te verwijderen. Wijzig regelmatig je wachtwoorden en loop privacy instellingen na op je telefoon en sociale media.

Als het je overkomt

Meld het

Meld doxing direct op je werk. Bespreek het incident ook met je collega's.

Zoek steun

Zoek steun bij familie, vrienden, collega's, lotgenoten of een bedrijfsopvangteam.

Aangifte doen

Wil je aangifte doen bij de politie? Als je wil kan je werkgever dit voor jou doen.

Bewijsmateriaal

Kun je het verzamelen van bewijsmateriaal overlaten aan een ander? Doe dat bij voorkeur niet zelf.

Beveiliging

Wordt beveiliging geregeld? Dit kan impact hebben op jou en je naasten. Bespreek regelmatig wat het met je doet en of het nog nodig is.

En wat daarna?

Evalueer het incident

Bespreek samen met jouw leidinggevende en je teamleden hoe jullie van het incident kunnen leren.

Blijf steun zoeken

Doxing kan lang een onveilig gevoel geven waardoor je minder plezier in je werk kan hebben. Zoek steun bij familie, vrienden, collega's, lotgenoten of een bedrijfsopvangteam als jouw stress weer toeneemt. Ook als anderen het incident alweer zijn vergeten.

ARQ Nationaal Psychotrauma Centrum

Nienoord 5
1112 XE Diemen
088 330 51 75

impact@arq.org
www.arq.org

Taskforce
Onze hulpverleners veilig