

Stappenplan voor aanschaf en implementatie van een **centraal getroffenregistratiesysteem** in Nederland

Stappenplan voor aanschaf en implementatie van een centraal getroffenregistratiesysteem in Nederland

RIVM-briefrapport 2026-0102

Colofon

© RIVM en NIPV 2026

Delen uit deze publicatie mogen worden overgenomen op voorwaarde van bronvermelding: Rijksinstituut voor Volksgezondheid en Milieu (RIVM) en Nederlands Instituut Publieke Veiligheid (NIPV), de titel van de publicatie en het jaar van uitgave.

DOI 10.21945/RIVM-2026-0102

F. de Zwart (auteur), RIVM
C. Cools (auteur), NIPV
A. Barrett (auteur), NIPV
M. Nachenius (auteur), NIPV
M. Pijnappel (auteur), RIVM
I. Rienstra (auteur), RIVM
L. Essink (auteur), RIVM

Contact:
Femke de Zwart
Gezondheid, Leefomgeving en Nazorg
femke.de.zwart@rivm.nl

Deze rapportage werd opgesteld in opdracht van het Ministerie van Volksgezondheid, Welzijn en Sport en het Ministerie van Justitie en Veiligheid in het kader van de opdrachtverstrekking voor een vervolg op de verkenning van de (on)mogelijkheden van centrale getroffenregistratie.

Deze uitgave komt voort uit een samenwerking tussen RIVM en NIPV

Rijksinstituut voor Volksgezondheid en Milieu

Postbus 1 | 3720 BA Bilthoven
Nederland
www.rivm.nl

Nederlands Instituut Publieke Veiligheid

Postbus 7010 | 6801 HA Arnhem
Nederland
www.nipv.nl

Publiekssamenvatting

Stappenplan voor aanschaf en implementatie van een centraal getroffenregistratiesysteem in Nederland

Bij rampen en crises is het voor de verschillende hulpdiensten en gemeenten lastig om snel te weten welke mensen erdoor getroffen zijn. Een landelijk registratiesysteem helpt hen om sneller te kunnen reageren, mensen beter te ondersteunen en zo de impact van een ramp te beperken. Een landelijk systeem hiervoor heeft veel voordelen en het is mogelijk om dat in Nederland op te zetten. Dat bleek eerder uit een verkenning naar de (on)mogelijkheden van centrale getroffenregistratie in Nederland.

In dit vervolg zijn een aantal zaken verder uitgewerkt. Zoals de voordelen van een getroffenregistratiesysteem, de privacyregels en het stappenplan voor het vervolg.

Een landelijk systeem moet voldoen aan de privacyregels. Daarom is in kaart gebracht welke gegevens over getroffen personen minimaal nodig zijn voor zorg en ondersteuning, en mogen worden gebruikt en bewaard. Ook is bekeken wat er nog meer moet worden geregeld om aan de regels te voldoen. Zo zijn goede afspraken nodig over wie welke gegevens mag bekijken en hoe lang de gegevens moeten worden bewaard.

Het projectteam adviseert om het systeem te laten beheren door een externe organisatie, zodat het veilig en betrouwbaar is in het gebruik. Verder moet één landelijke partij de leiding krijgen en ervoor zorgen dat het goed wordt beheerd. De kosten zullen hoger zijn dan het systeem waarmee nu naasten worden geïnformeerd over de locatie van een gewond familielid. Maar het centrale systeem registreert ook andere groepen die erbij betrokken zijn, zoals ooggetuigen die niet gewond zijn of mensen die bijvoorbeeld geen onderdak meer hebben. Het heeft daarom veel voordelen voor de hele samenleving. De betrokken hulpdiensten en organisaties steunen het plan.

Het Nederlands Instituut Publieke Veiligheid (NIPV) en het Rijksinstituut voor Volksgezondheid en Milieu (RIVM) voerden de twee verkenningen uit. In de volgende stap gaan bestuurders samen beslissen over het plan, de kosten en het voorstel voor het beheer. Als zij akkoord zijn en beslissen om het systeem te gaan invoeren, kan de aanbesteding en bouw ervan beginnen.

Kernwoorden: registratie, rampen, crisis, getroffen personen, nazorg, zorg, hulpverlening, crisisbeheersing, bevolkingszorg, gezondheidsonderzoek

Synopsis

Step-by-step plan for acquiring and implementing a central registration system in the Netherlands for people affected by disasters and crises

During disasters and crises, the various emergency services and municipalities may find it difficult to determine quickly who has been affected. A national registration system helps them respond more quickly and provide better care and support to affected people, thereby limiting the impact of a disaster. Such a system offers many benefits and can be set up in the Netherlands. This was demonstrated in an earlier exploratory study of the possibilities and limitations of establishing a central registration system in the Netherlands for people affected by disasters and crises.

This follow-up project examines several aspects in greater detail, including the benefits of a registration system for affected people, privacy rules and a step-by-step plan for the next phase.

A national system must comply with privacy rules. This project therefore identified which data about affected people are necessary for care and support and may legally be used and retained. The study also examined what other arrangements are needed to comply with the rules. For example, there must be clear agreements on who may access which data and how long those data must be retained.

The project team recommends that the system be managed by an external organisation to ensure that it is secure and reliable in use. Furthermore, one national organisation must take the lead and ensure that the system is properly managed. Costs will be higher than those of the current system, which is used to inform relatives of the whereabouts of an injured family member. However, the central system would also register other groups involved, such as uninjured eyewitnesses or people who have been left without shelter. This offers many benefits to society as a whole. The emergency services and organisations involved are in favour of the plan.

The Netherlands Institute for Public Safety (NIPV) and the National Institute for Public Health and the Environment (RIVM) carried out the two exploratory studies. In the next step, the relevant decision-makers will jointly decide on the plan, the costs and the management proposal. If they agree and decide to implement the system, the tendering and development of the system can begin.

Keywords: registration, disasters, crisis, affected people, aftercare, care, emergency assistance, crisis management, population care, health research

Inhoudsopgave

Managementsamenvatting — 7

1 Inleiding en leeswijzer — 9

Deel A - Verdieping op de verkenning — 11

2 Maatschappelijke businesscase — 12

- 2.1 Getroffenen en verwanten — 12
- 2.2 Acute zorgverlening en GHOR — 13
- 2.3 Bevolkingszorg en nafase — 13
- 2.4 Publieke gezondheidszorg (psychosociale hulpverlening en gezondheidsonderzoek bij rampen) — 14
- 2.5 Crisisbeheersing/Veiligheidsregio's — 14
- 2.6 Algemene baten/opbrengsten — 15
- 2.7 Kosten en afweging — 15
- 2.8 Conclusie — 15

3 Juridische Quickscan — 16

- 3.1 Inleiding en werkwijze — 16
- 3.2 Rechtmatigheid - juridische grondslag — 16
- 3.3 Behoorlijkheid en transparantie — 17
- 3.4 Doelbinding — 18
- 3.5 Dataminimalisatie — 19
- 3.6 Juistheid — 22
- 3.7 Opslagbeperking - bewaartermijn — 23
- 3.8 Integriteit en vertrouwelijkheid — 24

4 Voorstel voor beheer applicatie, hosting en inbedding — 26

- 4.1 Inleiding — 26
- 4.2 Korte toelichting begrippen — 26
- 4.3 Externe ontwikkeling, beheer, hosting en applicatieondersteuning — 27
- 4.4 Scheiding regie en technisch beheer — 27
- 4.5 SaaS-overeenkomst — 28
- 4.6 Eigenaarschap en gebruikersovereenkomst — 29
- 4.7 Minimaal benodigde diensten — 29
- 4.8 Aandachtspunten en conclusies — 30

5 Beschrijving van Programma van Eisen op hoofdlijnen — 32

- 5.1 Deel A: Registreren (fysiek, digitaal), traceren en volgen — 32
- 5.2 Deel B: Systeembeheer en administratieve functies — 33
- 5.3 Deel C: Informeren en communiceren — 34

Deel B - Stappenplan en aanbevelingen — 36

6 Stappenplan voor fase 3 en verder — 37

- 6.1 Fase 3: Voorbereiding op aanbesteding (3-6 maanden) — 37
- 6.2 Fase 4: Uitvoering van aanbesteding (5-10 maanden) — 38
 - 6.2.1 Publicatie (1-2 weken) — 39
 - 6.2.2 Vragenronde(s) - Nota van Inlichtingen (4-8 weken) — 39
 - 6.2.3 Indienen van inschrijvingen (6-10 weken) — 39

6.2.4	Beoordeling van inschrijvingen (6-12 weken) — 39
6.2.5	Voornemen tot gunning (20 dagen) — 40
6.2.6	Contractering (2-8 weken) — 40
6.3	Fase 5: Ontwerpen en testen van beoogd systeem (5 - 10 maanden) — 41
6.4	Fase 6: Acceptatie en implementatie van beoogd systeem (3 - 6 maanden) — 41
6.5	Fase 7: Borging en doorontwikkeling beoogd systeem — 42
6.6	Tijdslijn samengevat — 43

7 Conclusies, bestuurlijke besluitvorming en aanbevelingen — 44

7.1	Conclusies — 44
7.2	Bestuurlijke besluitvorming — 44
7.3	Aanbevelingen ten behoeve van het beoogde systeem — 45

Literatuur — 47

Verklarende woordenlijst — 48

Bijlage 1 Lijst met minimaal benodigde middelen/diensten van leverancier — 51

Bijlage 2 Lijst van functionaliteiten en onderdelen voor het Programma van Eisen op hoofdlijnen — 52

Managementsamenvatting

De voorliggende rapportage is een vervolg op de verkenning naar de (on)mogelijkheden van centrale getroffenenenregistratie in Nederland waarvan de resultaten in juni 2026 zijn gepubliceerd. Na de verkenningsfase is een tweede fase - opgesplitst in twee delen - opgestart. Fase 2a omvat deze rapportage, waarin alle benodigde zaken voor de voorbereiding op een aanbesteding én de besluitvorming op bestuurlijk niveau worden beschreven. Fase 2b omvat het bestuurlijk en financiële besluitvormingstraject en wordt op moment van schrijven nog doorlopen.

De voorliggende rapportage is opgedeeld in twee delen:

- Deel A; dit deel geeft een verdieping op de informatie die is opgehaald in de verkenningsfase en bevat de maatschappelijke businesscase, de juridische quickscan, het voorstel voor beheer, hosting en inbedding van de applicatie, en een Programma van Eisen op hoofdlijnen (hoofdstuk 2 t/m 5).
- Deel B; waarin het stappenplan om te komen tot een centraal getroffenenenregistratiesysteem in grote lijnen is uitgetekend (hoofdstuk 6). Daarnaast worden conclusies en aanbevelingen beschreven in hoofdstuk 7.

De maatschappelijke businesscase laat zien dat een centraal getroffenenenregistratiesysteem meerwaarde biedt in de vorm van efficiëntere werkprocessen, het voorkomen van maatschappelijke schade, het verbeteren van zorg en ondersteuning aan getroffenenen en het versterken van het vertrouwen in overheidshandelen bij rampen en crises. Het heeft een grote maatschappelijke meerwaarde.

De 'juridische quickscan' bevestigt nogmaals dat centrale getroffenenenregistratie binnen de kaders van de AVG mogelijk is, mits aan specifieke voorwaarden wordt voldaan. Kernbeginselen waarmee rekening moet worden gehouden, zoals rechtmatigheid, behoorlijkheid en transparantie, doelbinding, dataminimalisatie, juistheid, opslagbeperking, integriteit en vertrouwelijkheid, zijn verder uitgewerkt in het kader van de getroffenenenregistratie. Aangezien het projectteam in deze fase slechts kan uitgaan van een aantal uitgangspunten, zal een privacy scan in het vervolgtraject nogmaals moeten gebeuren middels een DPIA. Op dat moment zijn er in gesprek met stakeholders meer keuzes gemaakt over noodzakelijke gegevensverwerkingen en details in het ontwerp van de applicatie. Medische gegevens, net als BSN-nummers, worden in beginsel niet opgenomen, omdat deze niet noodzakelijk zijn voor de doelstellingen van het systeem. Daarnaast moeten duidelijke afspraken worden gemaakt over bewaartermijnen, rollen en rechten en beveiliging.

Voor het beheer en de hosting van het beoogde systeem wordt voorgesteld om te kiezen voor een SaaS (Software as a Service) overeenkomst met extern technisch beheer bij een gespecialiseerde leverancier. Voor de regie op het systeem heeft het de voorkeur om hier één centrale landelijke partij voor aan te wijzen. Deze inrichting heeft

voordelen op het gebied van robuustheid, professionaliteit, schaalbaarheid en uniformiteit, maar vereist wel een stevig ingerichte governance en een Programma van Eisen dat contractuele afspraken en verantwoordelijkheden helder weergeeft. In de voorliggende rapportage is een Programma van Eisen *op hoofdlijnen* opgenomen. Hierin worden de eerste functionele, technische en organisatorische vereisten beschreven. In de volgende fase volgt een gedetailleerdere versie van het Programma van Eisen en zal gewerkt worden aan de overige aanbestedingsdocumenten.

Voor doorgang naar fase 3 zijn vier randvoorwaarden bepalend: inhoudelijk draagvlak, gezamenlijk opdrachtgeverschap, structurele financiering en een heldere inrichting van de projectorganisatie en governance. Het inhoudelijk draagvlak wordt vastgesteld aan de hand van het bestuurlijk commitment van de zogenoemde 'kritieke massa'; de stakeholders die cruciaal voor succesvolle implementatie en gebruik van het beoogde getroffenregistratiesysteem. Om te komen tot het centraal getroffenregistratiesysteem zal een gefaseerde implementatie moeten worden gevolgd via aanbesteding, naar ontwikkeling, testen, implementatie en borging.

De uitkomsten van fase 2a laten zien dat een centraal getroffenregistratiesysteem zowel technisch, juridisch als organisatorisch haalbaar is en een duidelijke maatschappelijke meerwaarde heeft. Voor succesvolle realisatie is het essentieel dat in fase 2b bestuurlijk commitment wordt verkregen en afspraken worden gemaakt over financiering, governance en opdrachtgeverschap. Bij positief besluit tot voortgang, kan in fase 3 worden gestart met de voorbereiding op aanbesteding.

1 Inleiding en leeswijzer

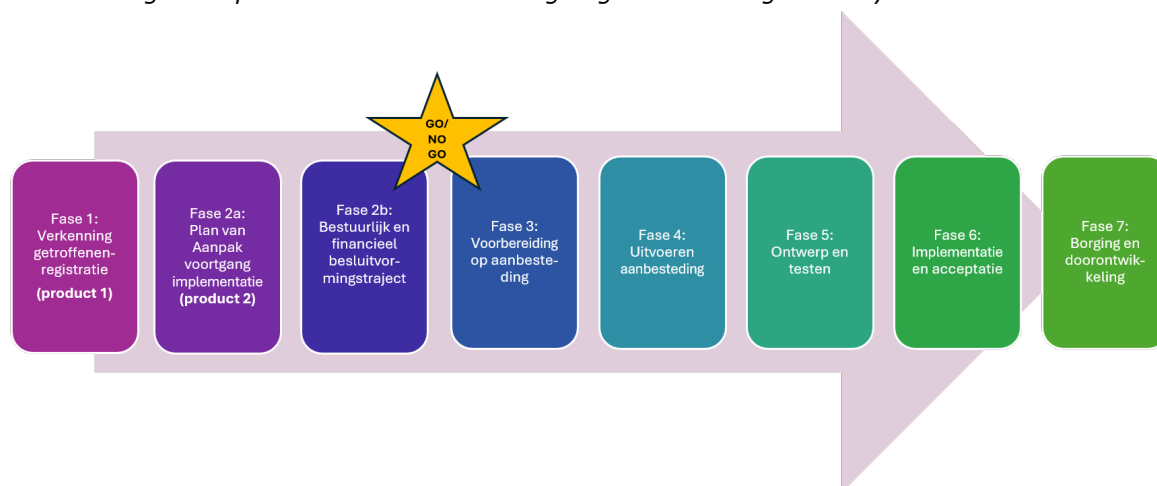
In juni 2026 is de rapportage van de resultaten van de 'Verkenning van de (on)mogelijkheden van centrale getroffenregistratie in Nederland' gepubliceerd. Uit deze verkenning blijkt dat er breed draagvlak is binnen de gehele keten (van zorg en ondersteuning aan getroffen) voor de implementatie van een centraal getroffenregistratiesysteem, mits privacy zorgvuldig geborgd is, werkprocessen vereenvoudigd worden en er een zelfregistratiemodule beschikbaar gesteld wordt. Deze verkenning liet tevens zien dat het beoogde registratiesysteem ook een oplossing zou kunnen bieden voor de huidige SIS applicatie die toe is aan vervanging. Op basis van de verkenning is besloten om een vervolg te geven aan de verkenning in de vorm van een tweede fase, waarvan de resultaten in deze rapportage zijn beschreven.

Deze tweede fase omvat een aantal zaken die noodzakelijk zijn voor de voorbereiding op de besluitvorming over de doorgang naar de volgende fase en de daaropvolgende aanbesteding; een stappenplan voor het vervolg, een voorstel voor beheer en hosting en een beschrijving van de maatschappelijke businesscase. Daarnaast biedt het een verdieping op de verkenning in fase 1. Zo is het onderdeel van de privacy kaders verder uitgewerkt in de 'juridische quickscan'.

Opsplitsing fase 2 in fase 2a en 2b

Naast deze inhoudelijke voorbereidingen op fase 3 is het ook nodig om een regievoerder aan te stellen, bestuurlijk commitment op te halen bij relevante stakeholders en afspraken te maken over de financiering van structurele en incidentele kosten. Zonder financiering heeft doorontwikkeling van plannen en aanbesteding weinig nut. Om die reden is ervoor gekozen om de oorspronkelijke fase 2 op te delen in twee delen: 2a en 2b. Fase 2a omvat deze rapportage, waarin alle benodigde zaken voor de voorbereiding op een aanbesteding én voor de besluitvorming op bestuurlijk niveau worden beschreven. Fase 2b omvat het bestuurlijk en financiële besluitvormingstraject. Fase 2b wordt getrokken door de stuurgroep met ondersteuning van de huidige projectgroep.

Figuur 1.1 Fasen in het proces van verkenning, besluitvorming, aanschaf, ontwikkeling en implementatie van het beoogde getroffenregistratiesysteem



Aanpak fase 2a

Om de voorliggende rapportage op te stellen zijn een aantal activiteiten uitgevoerd. De maatschappelijke businesscase is opgesteld aan de hand van de gesprekken die het projectteam in fase 2a gevoerd heeft met de betrokken stakeholders. De verwachte maatschappelijke baten zijn beschreven in het hoofdstuk van de maatschappelijke businesscase. De aanbevelingen op juridische vlak zijn opgesteld aan de hand van een 'juridische quickscan', uitgevoerd door een jurist en privacy-coördinator van het RIVM. De beschrijving van applicatiehosting en organisatorische inbedding is gebaseerd op gesprekken met betrokken partijen en ervaringen met bestaande systemen, waaronder SIS en het LCMS. Het concept Programma van Eisen (op hoofdlijnen) is opgesteld op basis van eerdere marktconsultaties rondom SIS, wensen vanuit de verschillende stakeholders en inzichten en ervaringen vanuit het BITS-systeem. Op basis van de resultaten in deze rapportage, de rapportage van de verkenning van de (on)mogelijkheden van centrale getroffenregistratie en de ervaringen met eerdere aanbestedingstrajecten is tenslotte ook een voorstel voor een stappenplan voor het vervolg gedaan.

Leeswijzer

Deze rapportage is opgebouwd in twee delen. In deel A is de verdieping op de verkenning beschreven met daarin de maatschappelijke businesscase (hoofdstuk 2), de juridische quickscan (hoofdstuk 3), het voorstel voor beheer applicatie, hosting en inbedding (hoofdstuk 4), en de beschrijving van het Programma van Eisen op hoofdlijnen (hoofdstuk 5).

In deel B van de rapportage zijn het proces om te komen tot een getroffenregistratiesysteem in grote lijnen uitgetekend. Hoofdstuk 6 beschrijft de stappen die gezet moeten worden vanaf fase 3. Daarna volgen enkele conclusies en aanbevelingen aan de stuurgroep en toekomstige projectorganisatie (hoofdstuk 7).

Deel A - Verdieping op de verkenning

2 Maatschappelijke businesscase

De implementatie van een centraal getroffenensysteem levert aanzienlijke maatschappelijke baten op voor verschillende stakeholdergroepen binnen en rondom de crisisbeheersing. De meerwaarde zit zowel in snellere en betere informatievoorziening als efficiëntere werkprocessen en het beperken van maatschappelijke en psychosociale schade.

In dit hoofdstuk worden de maatschappelijke voordelen en/of besparingen per stakeholder of proces beschreven.

2.1 Getroffenen en verwanten

Tijdige, juiste informatie

Voor getroffen en hun verwanten is tijdige, juiste en betrouwbare informatie van cruciaal belang (Rooze et al., 2009, p.104). Door directe en centrale registratie kan de matching van slachtoffers aan verwanten sneller en betrouwbaarder plaatsvinden (Ivankovic, EUCVT 2024, p.10). Verwanten ontvangen daardoor eerder duidelijkheid over de situatie van hun dierbare, wat onnodige onzekerheid, stress, miscommunicatie en verwarring aanzienlijk vermindert.

Betere, snellere psychosociale ondersteuning en zorg

Doordat het systeem niet alleen acute slachtoffers, maar juist de bredere groep van getroffen in beeld brengt, wordt het mogelijk om zorg en ondersteuning beter af te stemmen op individuele behoeften. Tijdige, passende en laagdrempelige ondersteuning (en zorg) zorgen ervoor dat eventuele mentale klachten niet onnodig verergeren en dat draagt bij aan het beperken van de instroom in de specialistische GGZ. Dit helpt bij de wachttijdproblematiek en voorkomt extra zorgkosten.

Voorkómen van secundaire stressoren

Daarnaast draagt beter gecoördineerde en passende ondersteuning in de nafase bij aan het voorkomen van een zogenaamde 'second disaster' (Gersons, 2020, p.4) of 'ramp na de ramp' (Nederlands Instituut Publieke Veiligheid, 2025). Overheidshandelen kan in het slechtste geval namelijk ook zorgen voor secundaire stressoren (Lock et al., 2012) die de impact van een ramp of crisis verder vergroten, herstel vertragen en uiteindelijk leiden tot hogere kosten en dalend vertrouwen in de overheid (bijvoorbeeld Groningse gaswinningsproblematiek en de toeslagenaffaire). Door meer volledige en centrale registratie sluit psychosociale zorg beter aan op de daadwerkelijke behoeften van getroffen, waardoor de kans op langdurige klachten afneemt.

Borging van privacy

Het nieuwe systeem voorziet ook in een verbetering van de AVG-compliance. In de huidige praktijk wordt er veelal gebruik gemaakt van mondelinge overdracht, niet altijd goed beschermde mails en zit er geen tot weinig controle op de toegang van de informatie (wie de informatie hoort of leest). Met het beoogde nieuwe systeem worden de persoonsgegevens beter beveiligd, is de toegang tot de informatie

gecontroleerd en wordt de noodzaak tot het versturen van mails met gevoelige informatie weggenomen. Dit verkleint de kans op datalekken en draagt bij aan het vertrouwen van burgers in de overheid als zorgvuldige gegevensverwerker.

2.2 Acute zorgverlening en GHOR

Voor de acute zorgpartijen en de GHOR levert het systeem efficiëntiewinst op. Het handmatig uitvragen en soms ook overdragen van slachtoffergegevens bij de OvD-G, de ambulances, de ziekenhuizen en de gewonden-verzamellocatie, het mailen van bestanden en het dubbel invoeren in eigen systemen vervalt. In plaats daarvan is direct een actueel, accurater en vollediger overzicht beschikbaar. Dit bespaart de ambulance, ziekenhuizen en GHOR tijd en capaciteit tijdens de crisis.

Het overzicht van het aantal slachtoffers en hun triageclassificatie stelt de meldkamer in staat slachtoffers sneller en effectiever over ziekenhuizen te spreiden. Bovendien komen de handmatige handelingen die hier voorheen voor nodig waren (doorbellen of mailen tussen ziekenhuizen en GHOR) hiermee te vervallen. Hierdoor wordt er tijd, capaciteit en kosten bespaard tijdens de ramp of crisis.

2.3 Bevolkingszorg en nafase

Het implementeren van een centraal getroffenregistratiesysteem levert duidelijke maatschappelijke meerwaarde op voor de bevolkingszorg, zowel in de acute fase als in de nafase. In de huidige situatie zijn registratie, informatiedeling en opvolging van getroffen versnipperd over meerdere organisaties en systemen. Dit leidt tot onvolledige overzichten, dubbele registraties en verhoogde foutgevoeligheid. Als gevolg daarvan zijn getroffen, met name in de nafase, niet altijd volledig in beeld en komt zorg, ondersteuning of informatie soms te laat of niet bij de juiste personen terecht. Dit vergroot de belasting voor hulpverleningsorganisaties, gemeenten en zorginstellingen en kan maatschappelijke schade versterken, bijvoorbeeld door onrust bij verwanten, vertraging in psychosociale ondersteuning en het onvoldoende signaleren van gezondheidsklachten.

Een centraal systeem maakt het mogelijk om informatie over getroffen sneller, vollediger en gerichter te delen tussen betrokken partijen. Voor de bevolkingszorg betekent dit een belangrijke verbetering, omdat zowel de acute inzet als de nafase beter wordt ondersteund.

Voor de SIS-organisatie biedt een centraal getroffenregistratiesysteem ook aanzienlijke voordelen. De huidige SIS-applicatie is aan vervanging toe en de SIS-processen kunnen worden ondersteund door het nieuwe systeem. De middelen die nu jaarlijks worden ingezet voor de SIS-programmaorganisatie kunnen worden benut voor het nieuwe systeem.

Hierdoor ontstaat de mogelijkheid om verwanten sneller en betrouwbaarder te informeren, doordat actuele informatie direct beschikbaar is, onder meer vanuit ziekenhuizen. Dit versnelt het matchen van verwanten met hun naasten en voorkomt dat verwanten op eigen initiatief naar rampgebieden of verschillende ziekenhuizen

gaan, op zoek naar informatie. Verwanten en naasten die naar de rampgebieden gaan kunnen de hulpverlening bemoeilijken en het leidt soms tot risico's voor de verwanten en naasten.

Voor gemeenten ontstaat in de nafase een beter overzicht van welke inwoners getroffen zijn, welke ondersteuning nodig is en waar risico's ontstaan op psychosociale of maatschappelijke problematiek. Dit maakt het mogelijk om nazorg en herstellzorg gericht, efficiënter en effectiever te organiseren.

2.4 Publieke gezondheidszorg (psychosociale hulpverlening en gezondheidsonderzoek bij rampen)

Doordat *alle* typen getroffen en beter in beeld zijn met het nieuwe systeem (o.a. door middel van zelfregistratie) en niet alleen de - niet-zelfredzame - slachtoffers die in zorg belanden, stelt het de gemeente en GGD beter in staat om deze getroffen ook te kunnen benaderen voor psychosociale hulpverlening (zie baten voor de getroffen) en/of gezondheidsonderzoek bij rampen.

Het registratiesysteem verbetert bovendien de basis van het gezondheidsonderzoek doordat de populatie getroffen volledig en betrouwbaarder is vastgelegd, wat zal leiden tot minder bias in de onderzoeksresultaten. Op basis van deze resultaten kunnen betrouwbaardere uitspraken gedaan worden over de (gezondheids)impact van een ramp of crisis en de zorg- en ondersteuningsbehoeften die leven. Het gezondheidsonderzoek heeft bovendien als neveneffect dat het tevens erkenning biedt aan getroffen, door te laten zien dat de overheid begaan is met het lot van getroffen. De resultaten van betrouwbaar gezondheidsonderzoek stellen de autoriteiten in staat om psychosociale hulpverlening beter aan te laten sluiten op de behoeften die leven, en daarmee beter te voldoen aan hun wettelijke taak om ondersteuning te bieden aan getroffen van rampen en crises.

2.5 Crisisbeheersing/Veiligheidsregio's

Voor de Veiligheidsregio/crisisbeheersing biedt het systeem betere en sneller beschikbare informatie op en over plaats incident. Hierdoor kunnen binnen het ROT (Regionaal Operationeel Team) sneller passende keuzes worden gemaakt. Wanneer bijvoorbeeld, in specifieke gevallen met grote branden en mogelijke meerdere betrokken burgers, sneller duidelijk wordt of er geen vermisten meer zijn met betrekking tot de brand, kan eerder worden overgegaan van redden naar bergen. Dit vermindert onnodige risico's voor hulpverleners.

Ook ondersteunt het systeem de crisiscommunicatie vanuit de Veiligheidsregio. Actueel inzicht in aantallen gewonden, getroffen, vermisten en overledenen stelt bestuurders beter in staat hun communicatie hierop af te stemmen. Duidelijke informatie helpt burgermeesters om hun rol als burgervader of -moeder richting de getroffen gemeenschap passend in te vullen.

2.6 Algemene baten/opbrengsten

In algemene zin geldt dat door de registratie op één centrale plek (en koppeling met andere systemen) vorm te geven er efficiënter gewerkt kan worden in de hele keten. Er zijn minder handmatige acties nodig, registraties hoeven niet meer op meerdere plekken plaats te vinden en de nauwkeurigheid van gegevens neemt toe. Dit leidt tot structurele tijdsbesparing en kwaliteitsverbetering.

Daarnaast zorgt zelfregistratie voor een beter beeld van het totaal aantal getroffen en. Hierdoor raken minder mensen uit beeld, wordt onnodig zoeken naar vermisten voorkomen en is de kans kleiner dat mensen geen hulp ontvangen terwijl ze die wel nodig hebben.

2.7 Kosten en afweging

Tegenover genoemde baten staan de kosten voor aanschaf, implementatie, beheer, scholing en exploitatie van het systeem. Deze kosten liggen aanzienlijk hoger dan de huidige kosten van SIS. Het nieuwe systeem bedient echter een bredere getroffen en doelgroep en meer verschillende doelstellingen dan het huidige SIS.

2.8 Conclusie

Deze investering zorgt voor meer zicht op getroffen en, snellere informatiedeling op bestuurlijk niveau en met naasten/verwanten en een snellere, betere (na)zorg waardoor er sneller herstel kan optreden en minder kans is op langdurige maatschappelijke schade.

De meerwaarde van het systeem zit niet alleen in efficiëntere werkprocessen, maar vooral in het voorkomen van genoemde maatschappelijke schade, het verbeteren van zorg en ondersteuning en het versterken van het vertrouwen in het overheidshandelen bij rampen en crises. Bij de inrichting van het systeem zijn duidelijke afspraken nodig over governance, financiering, beheer, privacy en rollen en rechten van gebruikers.

3 Juridische Quicksan

3.1 Inleiding en werkwijze

In het kader van de bescherming van de privacy van burgers is het van belang dat bij het verwerken, delen en bewaren van persoonsgegevens zorgvuldig te werk gegaan wordt. In fase 1 zijn de wettelijke kaders in kaart gebracht. De conclusie van deze verkenning is dat centrale getroffenregistratie wettelijk toegestaan is, mits aan een aantal randvoorwaarden wordt voldaan. De wettelijke kaders bepalen welke gegevens, wanneer en met welke grondslag mogen worden verwerkt, gedeeld en bewaard. Omdat het getroffenregistratiesysteem nog ontwikkeld moet worden kan een DPIA (*Data Protection Impact Assessment*) op dit moment nog niet uitgevoerd worden. Om inzicht te verkrijgen in belangrijke aandachtspunten voor het ontwerp, hebben we een 'juridisch quickscan' laten uitvoeren door enkele juristen en privacy coördinatoren. Deze experts hebben de inhoudelijke uitgangspunten (zoals geformuleerd in fase 1) voor het ontwerp van het systeem getoetst aan de (AVG-)regelgeving. De resultaten van deze quickscan en eventuele aandachtspunten staan aan de hand van de algemene beginselen van de AVG beschreven in dit hoofdstuk. Vanwege het feit er nog veel zaken verder uitgewerkt moeten worden in het vervolgtraject, is het wenselijk om (naast een privacy coördinator) een vaste (privacy- en gezondheids-) jurist te betrekken in het projectteam die het proces van het begin tot einde kan begeleiden.

3.2 Rechtmatigheid – juridische grondslag

Rechtmatigheid is een van de kernbeginselen van de AVG; persoonsgegevens mogen niet zomaar verwerkt worden, er moet altijd een juridische grondslag zijn. Ook mag de registratie van persoonsgegevens niet in strijd zijn met andere wetgeving, zoals bijvoorbeeld de wettelijke geheimhoudingsplicht.

De grondslagen voor verwerking van persoonsgegevens kunnen volgens artikel 6 van de AVG de volgende zijn: toestemming, uitvoering van een overeenkomst, wettelijke verplichting, vitaal belang van betrokkene of andere personen, de vervulling van een taak van algemeen belang of de uitoefening van openbaar gezag en gerechtvaardigd belang.

Afhankelijk van wie verantwoordelijk wordt voor de verwerkingen en wie de verwerkingen uitvoert, kunnen verschillende grondslagen van toepassing zijn voor de verwerking. Zo kan de grondslag van vervulling van een taak van algemeen belang of de uitoefening van openbaar gezag (artikel 6 lid 1 sub e AVG) mogelijk van toepassing zijn. De grondslag voor verwerking dient in het vervolgtraject per verwerkingsverantwoordelijke of verwerker en per specifieke verwerking beoordeeld te worden. De hieronder uitgewerkte grondslagen zijn in ieder geval van belang bij de verwerkingen in relatie tot de doelstellingen van de centrale getroffenregistratie.

Met betrekking tot de registratie van persoonsgegevens van direct getroffen van een ramp of crisis kan een beroep gedaan worden op een **vitaal belang**, als bedoeld in artikel 6 lid 1 sub d van de AVG. De verwerking is noodzakelijk om de vitale belangen van de betrokkene of van een andere natuurlijke persoon te beschermen. Alleen op die manier kan namelijk de noodzakelijke hulpverlening onmiddellijk en adequaat worden opgestart. In die situatie is het onmogelijk om eerst alle betrokkenen te informeren en toestemming te vragen om hun persoonsgegevens te kunnen verwerken. Dit geldt ook voor personen die wilsonbekwaam of minderjarig zijn.

Het gebruik van het getroffenregistratiesysteem wordt ook afgebakend tot gebruik in noodsituaties, en dient niet voor reguliere werkzaamheden van de betrokken partijen die gebruik zullen maken van het getroffenregistratiesysteem.

Indien getroffen die lichtgewond zijn of getuigen zijn van de situatie zichzelf registreren, kan het vitale belang onvoldoende grondslag bieden. In dat geval dient toestemming (artikel 6 lid 1 sub a AVG) als grondslag voor de verwerking.

Met betrekking tot de registratie van verwanten dient er, conform het bepaalde in artikel 6 lid 1 sub a van de AVG, sprake te zijn van **toestemming** van de verwant. De verwanten moet expliciet toestemming geven voor de verwerking van zijn/haar gegevens voor een of meerdere specifieke doeleinden.

In het kader van ondersteuning en zorg aan getroffen is het ook noodzakelijk om in specifieke situaties bijzondere persoonsgegevens te registreren, zoals de nationaliteit van buitenlandse getroffen. Omdat buitenlandse ambassades geïnformeerd moeten worden over de getroffen uit hun land, is het van belang om deze gegevens te registreren. In principe is het verboden om bijzondere persoonsgegevens te verwerken tenzij er sprake is van bepaalde uitzonderingsregels, zoals de expliciete toestemming of het vitale belang (artikel 9 lid 2 AVG). Deze uitzonderingsgronden kunnen ook hier van toepassing zijn. Voor de verwerking van bijzondere persoonsgegevens zal in het vervolgtraject moeten worden vastgesteld welke uitzonderingsgronden daadwerkelijk van toepassing zijn.

3.3 Behoorlijkheid en transparantie

Behoorlijkheid betekent dat gegevensverwerking niet misleidend, oneerlijk of onrechtvaardig mag zijn voor de betrokkene. Organisaties moeten duidelijk, open en eerlijk (transparant) zijn over hoe zij de persoonsgegevens verwerken (artikelen 12, 13 en 14 AVG).

In het beoogde registratiesysteem worden gegevens geregistreerd van getroffen, verwanten en vermisten¹ van rampen, crises en incidenten. In principe is het uitgangspunt dat dat getroffen en verwanten expliciet om toestemming gevraagd zal worden alvorens hun persoonsgegevens verwerkt zullen worden. Op het moment dat toestemming gevraagd wordt zal ook uitgelegd worden waar de

¹ Zie definities in de begrippenlijst.

gegevens voor gebruikt worden, met wie deze gedeeld worden en hoe lang deze bewaard worden. Met een goede privacyverklaring wordt tegemoetgekomen aan de informatieplicht.

Ook wanneer een getroffene zichzelf in het systeem registreert via een registratiemodule op een website, zal de privacyverklaring daar expliciet onder de aandacht gebracht worden.

Een getroffene kan indien gewenst ook een uitdraai van zijn/haar/hun registratiedossier opvragen, en/of een verzoek indienen om zijn persoonsgegevens te verwijderen uit het registratiesysteem (opt-out).

Voor de gevallen waarin de betrokkene niet vooraf geïnformeerd kon worden, bijvoorbeeld gezien de staat waarin de betrokkene verkeerde, wordt op een later moment alsnog getracht tegemoet te komen aan de informatieplicht wanneer de betrokkene in staat is om deze informatie tot zich te nemen.

Wat betreft het nazorg doel, wordt voorafgaand aan de informatiedeling met nazorgprofessionals toestemming gevraagd voor de verwerkingen van persoonsgegevens, op een moment wanneer de betreffende getroffene in staat is om de informatie tot zich te nemen en toestemming te geven.

3.4 Doelbinding

Doelbinding houdt in dat persoonsgegevens alleen mogen worden verzameld voor een 'welbepaald, uitdrukkelijk omschreven en gerechtvaardigd' doel.

Het beoogde getroffenenenregistratiesysteem richt zich op het lokaliseren, identificeren en traceren van getroffenenen tijdens een incident, ramp of crisis (van een zekere omvang) zodat adequate hulpverlening (zorg en ondersteuning) kan worden opgestart en partners aan hun wettelijke taken kunnen voldoen.

Het beoogde getroffenenenregistratiesysteem zou in elk geval de volgende doelen moeten dienen:

- Betrouwbaar overzicht creëren van aantal en classificatie van getroffenenen en verder benodigde informatie ten behoeve van de organisatie van de geneeskundige hulpverlening;
- Informeren van bevoegd gezag, overheidsinstanties en (hulp)diensten die betrokken zijn bij de crisisbeheersing, zoals de burgemeester van een gemeente, de veiligheidsregio, ambassades en/of de ministeries van JenV en VWS;
- Gericht afstemmen van de psychosociale hulpverlening tijdens de *acute fase* en de *nafase* van een ramp, crisis of incident;
- Verzamelen van gegevens noodzakelijk voor het gericht opvolgen van zorg- en ondersteuningsbehoeften van getroffenenen (in het kader van Bevolkingszorg en Psychosociale hulpverlening) in de *acute fase en nafase* van een ramp, crisis of incident;

- Informeren van verwanten over de locatie van de niet-zelfredzame getroffen en (die zelf niet in staat zijn om hun verwanten te informeren);
- Herenigen van getroffen en met hun verwanten en naasten;
- Verzamelen van gegevens noodzakelijk ten behoeve van het verrichten van gezondheidsonderzoek bij rampen en crises, om de gezondheidsimpact in kaart te kunnen brengen en beleid hierop af te kunnen stemmen.

Bij de laatste doelstelling gaat het er hoofdzakelijk over dat het systeem de met deze taak belaste professionals in staat stelt om de getroffen en te kunnen benaderen voor een verzoek om deelname aan het gezondheidsonderzoek. In het systeem zullen *geen* gegevens geregistreerd worden die in het onderzoek verzameld zijn. Hiervoor zullen de professionals hun eigen processen en systemen gebruiken.

3.5 Dataminimalisatie

In het kader van dataminimalisatie is het van belang dat in het beoogde registratiesysteem alleen die gegevens genoteerd worden die essentieel zijn voor het kunnen lokaliseren, identificeren en traceren van getroffen en, verwanten en vermisten, om zo aan de doelstellingen te voldoen.

De uitgebreidheid van de gegevens die minimaal moet worden geregistreerd varieert op basis van de locatie waar de getroffene zich op het moment van registratie bevindt. Uit de verkenning blijkt dat er in de acute fase primair behoefte is aan de locatie, datum en tijdstip van het incident in aanvulling op de triageclassificatie (T1-T3), de (geschatte) leeftijd en geslacht van de persoon. In een levensbedreigende situatie **gaat de zorg voor getroffen en (T1 en T2-slachtoffers) altijd voor registratie**. De focus van de registratie ligt dan op de locatie en de ernst van de verwondingen.

De registratie wordt uitgebreid op die plaatsen waar de prioriteit niet (meer) ligt op levensreddende medische handelingen, zoals opvanglocaties of ziekenhuizen. Daarnaast kunnen licht- en niet-gewonden personen en verwanten zich vrijwel altijd zelf identificeren, en kunnen er dus meer gegevens genoteerd worden in het systeem.

Wat de overige benodigde gegevens zijn die in het systeem geregistreerd moeten worden is afhankelijk van de wettelijke taak van de verschillende stakeholders. Zo is het voor Bevolkingszorg en de PSH- en GOR-professionals van belang dat ook de NAW-gegevens van de persoon en de betrokkenheid bekend zijn, zodat zij gericht kunnen worden benaderd over hun zorg- en ondersteuningsbehoefte.

Vermoedelijk zijn de volgende zaken **wenselijk** om over de verschillende subdoelgroepen te registreren.

Tabel 3.1 Tabel met typen gegevens die wenselijk zijn om te registreren over de verschillende subdoelgroepen in het registratiesysteem

Type gegeven		Dossier		
No.	Gegeven	Getroffene	Verwant	Vermiste
1	Unieke code ¹	√	√	√
2	Naam ¹	√	√	√
3	Voornaam ¹	√	√	√
4	Betrokkenheid ¹	√	√	√
5	Triageclassificatie ¹	√		
6	Geschatte leeftijd ¹	√		
7	Geboortedatum ¹	√	√	√
8	Leeftijd ¹	√	√	√
9	Geslacht/gender ¹	√	√	√
10	Nationaliteit ¹	√		√
11	Land ¹	√	√	
12	Taal ¹	√	√	
13	Straatnaam ¹	√	√	
14	Huisnummer ¹	√	√	
15	Postcode ¹	√	√	
16	Woonplaats ¹	√	√	
17	Telefoonnummer 1 ¹	√	√	
18	Telefoonnummer 2	√	√	
19	E-mail ¹	√	√	
20	Vrij veld	√	√	√
21	Tijdelijke verblijfplaats	√	√	
22	Kan bij vrienden of familie overnachten	√		

Type gegeven		Dossier		
No.	Gegeven	Getroffene	Verwant	Vermiste
23	Afdeling ziekenhuis	√		
24	Aanvrager	√*	√*	
25	Op zoek naar vermiste	√*	√*	
26	Band met vermiste	√*	√*	
27	Wordt gezocht door			√*
28	Vermiste teruggevonden			√*
29	Vermiste teruggevonden – vrije tekst			√*
30	Tijdstip van zelfregistratie	√	√	
31	Gemeld	√*	√*	
32	Type registratiepunt	√	√	
33	Huidige locatie	√	√	
34	Bestemming	√		
35	Hulpverlening verlaten	√	√	
36	Tijdstip IN	√	√	
37	Tijdstip UIT	√	√	
38	Tijdstip oproep SIS frontoffice	√	√	
39	Traject	√	√	
40	Foto	√	√	
41	Familie verband	√*	√*	

In geval van gewonde, niet-zelfredzame getroffenen (slachtoffers), die naar een ziekenhuis vervoerd worden, wordt er aanvullend nog een aantal zaken geregistreerd ikhv verwanteninformatie.

¹ Minimaal wenselijke informatie over getroffenen

* Deze gegevens zijn gekoppeld aan het andere dossier

Bij grootschalige gebeurtenissen met een groot aantal overledenen en/of vermisten moet het mogelijk kunnen zijn om **foto's van personen en opvallende uiterlijk kenmerken** te uploaden in het registratiesysteem om de identificatie van personen te ondersteunen. Vanwege de privacy van de getroffene zullen deze foto's moeten worden afgeschermd (alleen als je er echt bewust voor kiest om een pop-up scherm weg te klikken krijg je een foto te zien), en is inzien alleen voorbehouden aan aangewezen functionarissen werkzaam in het proces van de verwanteninformatie.

We adviseren om in principe **géén medische gegevens te registreren** in het dossier van een getroffene. Het is een getroffenregistratiesysteem, en geen medisch registratiesysteem. Dergelijke registratie is voorbehouden aan BIG geregistreerde hulpverleners die, in het kader van de WGBO, een behandelovereenkomst aangaan met betreffend persoon. Belangrijker, medische gegevens uit het medische dossier van een individu zijn niet noodzakelijk voor de doeleinden van lokaliseren, traceren en identificeren. Inzicht in de triageclassificatie op geaggregeerd niveau is wél noodzakelijk om het bevoegd gezag binnen de rampenhulpverlening te informeren, en is naar verwachting wel toegestaan binnen bestaand juridisch kader.

Bovendien is er voor het registreren van medicatietoedieningen op plaats incident momenteel al een bewezen effectieve werkwijze beschikbaar (noteren ervan op witte polsbandjes), waarmee de 'noodzakelijkheid' van de registratie van deze gegevens eigenlijk wat verloren raakt. Hiermee wordt het opnemen van deze gegevens in het kader van de AVG moeilijker verdedigbaar.

In het vervolgtraject zal dus nog meer duidelijkheid moeten worden verschaft over welke gegevens strikt **noodzakelijk** zijn voor de omschreven verwerkingsdoelen, waardoor een definitieve lijst van te verwerken persoonsgegevens kan worden opgesteld. In de in het vervolgtraject op te stellen DPIA wordt hier uitgebreid aandacht aan besteed.

Daarnaast zijn ook de gegevens die geregistreerd worden van gebruikers van het systeem, wanneer zij data invoeren of bekijken, onderhevig aan de AVG-regelgeving als het gaat om verwerkingen van persoonsgegevens. Dit zal ook in de DPIA meegenomen moeten worden in de lijst van gegevens die verzameld zullen worden.

3.6 Juistheid

Juistheid in het kader van de AVG gaat over het feit dat de persoonsgegevens die geregistreerd kloppend moeten zijn en dat de betreffende persoon om een rectificatie moet kunnen vragen. Met een toekomstig systeem wordt een goede bijdrage geleverd aan de juistheid van de gegevens.

Voor het behalen van de doelstellingen is het ook van belang dat personen geregistreerd kunnen worden zonder dat ze geïdentificeerd zijn. Wanneer gewonden op plaats incident aangetroffen worden zonder

identificatie zal de acute hulpverlening toch zorg gaan verlenen. Identificatie zal dan later plaatsvinden. Door het registreren van ongeïdentificeerden zorgen we ervoor dat deze mensen wel in het overzicht meegenomen worden en niet onder meerdere verschillende namen/aanduidingen op de lijst verschijnen. Het verkleint de foutgevoeligheid. Bij registratie krijgen alle personen een uniek nummer op een polsbandje of iets dergelijks dat aan de persoon gehecht zit. Hiermee wordt gewaarborgd dat op alle locaties waar deze persoon komt, het juiste dossier wordt aangevuld. Als de identiteit duidelijk is kan deze ook aan het juiste dossier toegevoegd worden. Uiteraard is het ook altijd mogelijk om aanpassingen te (laten) doen aan de registraties, in het geval er toch een fout in is geslopen. Op centraal niveau zal er een functionaris aangesteld worden die bevoegdheid heeft om dossiers te wijzigen, of eventueel samen te voegen wanneer een vermiste toch onder de getroffen personen geregistreerd wordt.

Voor de medische behandeling van een getroffen persoon zijn betrokken partijen (behandelaar(s), ziekenhuis, ambulancedienst) *verplicht* het BSN te verwerken. Registratie van BSN is echter voorbehouden aan specifieke partijen. Hoewel de behoefte om het BSN te verwerken in het registratiesysteem (om persoonsverwarring te voorkomen) begrijpelijk is, is het voor de doelstellingen van getroffenregistratie niet nodig en bovendien niet toegestaan voor de registrerende partijen. Het huidige overzicht aan te verwerken gegevens biedt hoogstwaarschijnlijk voldoende informatie om iemand als uniek persoon te registreren (naam, adres, woonplaats, geboortedatum etc.) en persoonsverwarring te voorkomen. Om deze redenen adviseren wij om geen BSN-nummers te registreren in het toekomstige systeem.

3.7 Opslagbeperking – bewaartermijn

In beginsel mogen de persoonsgegevens worden bewaard tot het moment waarop het doel waarvoor deze gegevens zijn verkregen is gerealiseerd of is opgehouden te bestaan, tenzij er een (aanvullende) wettelijke grondslag van toepassing is die bepaalt dat de persoonsgegevens langer of korter moeten worden bewaard. De verwerkingsverantwoordelijke dient erop toe te zien dat de persoonsgegevens tijdig worden vernietigd.

De juristen van JenV en NIPV hebben in het kader van SIS beoordeeld dat de bewaartermijn van de persoonsgegevens in het kader van de nazorg 6 weken is. Indien de 'nazorg' nog niet is afgerond - er is bijvoorbeeld nog gevraagd om toekomstige nazorg of er is nog een openstaande zoekvraag van een verwant - kunnen de persoonsgegevens maximaal 1 jaar langer worden bewaard. Deze verlenging is slechts een uitzondering op de regel. In de regel worden de persoonsgegevens maximaal 6 weken bewaard. Dit is begrijpelijk wanneer je bedenkt dat het opsporen van verwanten iets is van de acute fase van een ramp of crisis. Onder 'nazorg' wordt vanuit het proces van verwanteninformatie iets anders verstaan dan vanuit bevolkingszorg en psychosociale hulpverlening. Binnen de getroffenregistratie zijn de doelstellingen verbreed, en kan nazorg (in de vorm van bv opvolging van noden, herdenkingen, gezondheidsonderzoek, etc.) in deze context soms soms jaren duren.

In het kader van potentiële gezondheidsonderzoeksdoeleinden zal in een volgende fase ook nog gekeken moeten worden of anonimisering van de data een wenselijk en mogelijk alternatief is voor de vernietiging van bepaalde gegevens.

Voor het vervolgtraject is van belang dat in kaart wordt gebracht welke gegevens voor een langere tijd bewaard kunnen blijven in het kader van de langere nazorg. Hiertoe moet worden bepaald welke gegevens noodzakelijk zijn en dus bewaard mogen blijven en welke gegevens eventueel eerder verwijderd dienen te worden. De onderbouwing van de noodzakelijkheid van het langer bewaren van gegevens is daarvoor van cruciaal belang en zal in een DPIA verder uitgewerkt moeten worden.

3.8 Integriteit en vertrouwelijkheid

Aan de beveiliging van de gegevens zal (blijvend) uitgebreid aandacht worden besteed. Het systeem zal ook bijzondere persoonsgegevens bewaren, waardoor extra beveiliging noodzakelijk is. Een aantal zaken die nu al voorzien worden (o.a. in het ontwerp van een nieuw systeem):

- Adequate beveiliging van gegevens en toegang in het systeem
- Logging en auditing
- Afspraken maken over rollen, rechten en verantwoordelijkheden van de gebruikers
- Regionale toewijzing van autorisaties en periodieke controles op de autorisaties
- Technische beveiliging vanuit de beherende partij (zoals bv firewalls, gescheiden netwerken, etc.)
- Verwerkersovereenkomsten en samenwerkingsconvenanten
- Procedure voor de afhandeling van eventuele datalekken

De ondervraagde ketenpartners hechten groot belang aan het beschermen van de persoonsgegevens van getroffen personen binnen het beoogde systeem. Om ervoor te zorgen dat gebruikers geen inzicht krijgen in meer gegevens dan strikt noodzakelijk voor hun taak binnen de keten van (acute en/of psychosociale) zorg en ondersteuning, zullen rollen gedefinieerd moeten worden. Betrokken stakeholders kunnen één of meerdere rollen toegekend krijgen, die gepaard gaan met specifieke rechten en verantwoordelijkheden/taken. Zo kunnen ze bepaalde gegevens invoeren, inzien en/of functionaliteiten in het systeem gebruiken.

Uit de in het vervolgtraject op te stellen DPIA kunnen specifieke risico's en maatregelen om die risico's te beperken volgen. Daarnaast biedt de BIO (Baseline informatiebeveiliging Overheid) algemene kaders voor de beveiliging van gegevens. Het getroffen registratiesysteem zal aldus in ieder geval aan deze eisen moeten voldoen. In het vervolgtraject zal informatie ingewonnen moeten worden bij informatiebeveiligingsspecialisten en privacy experts om het volledige maatregelenpakket samen te stellen.

Ook zullen in het vervolgtraject verwerkersovereenkomsten en samenwerkingsafspraken gemaakt moeten worden die duidelijk omschrijven welke data door welke partijen uit het systeem gehaald mag worden voor specifieke verwerkingen. Dit geldt bijvoorbeeld voor het gezondheidsonderzoek bij rampen, waar gegevens uit het systeem benut zullen worden om, aangevuld met gegevens uit het onderzoek, een onderzoeksdatabase op te stellen. Afspraken moeten duidelijk maken welke gegevens wel en niet noodzakelijk zijn voor dit soort doelstellingen.

4 Voorstel voor beheer applicatie, hosting en inbedding

4.1 Inleiding

In dit hoofdstuk wordt een voorstel gedaan voor de inrichting van het beheer, de hosting en de organisatorische inbedding van het centrale getroffenregistratiesysteem. Het doel is om te komen tot een stabiele, veilige en toekomstbestendige oplossing die continu beschikbaar is, met name tijdens rampen en crises.

Daarbij wordt gekeken naar een passende verdeling van verantwoordelijkheden tussen de technische uitvoering, de hosting, de applicatieondersteuning en de landelijke regie op het systeem. Ook wordt ingegaan op de randvoorwaarden, voordelen en aandachtspunten van deze inrichting, zodat het systeem duurzaam kan worden beheerd en doorontwikkeld.

4.2 Korte toelichting begrippen

Met **beheer** wordt bedoeld: het geheel aan activiteiten dat nodig is om het systeem goed, veilig en actueel te laten functioneren. Denk hierbij aan technisch onderhoud, updates, gebruikers- en rollenbeheer, beveiliging, back-ups, monitoring en het oplossen van storingen.

Onder **hosting** wordt verstaan dat de applicatie en de bijbehorende gegevens worden ondergebracht in een technische omgeving, zoals servers en databases, zodat het systeem via internet beschikbaar is voor gebruikers. Hosting gaat daarmee over de technische infrastructuur, beschikbaarheid, beveiliging, opslagcapaciteit en prestaties van het systeem.

Met **applicatieondersteuning** wordt bedoeld: de ondersteuning aan gebruikers en beheerders bij het gebruik van het systeem. Hieronder vallen bijvoorbeeld een servicedesk voor vragen en incidenten, documentatie, ondersteuning bij wijzigingen, het beheer van updates en het begeleiden van gebruikers bij het goed toepassen van de applicatie.

Met **landelijke regie** wordt bedoeld dat één landelijke partij verantwoordelijk is voor de centrale sturing, bewaking en doorontwikkeling van het systeem. Deze partij voert niet per se zelf het technisch beheer uit, maar ziet erop toe dat het systeem aansluit bij de landelijke werkwijze, de behoeften van de gebruikers en de eisen die gelden binnen het crisisdomein.

Samen zorgen beheer, hosting, applicatieondersteuning en landelijke regie ervoor dat het getroffenregistratiesysteem betrouwbaar, veilig, uniform en continu beschikbaar is, ook tijdens rampen, crises en oefeningen.

4.3 Externe ontwikkeling, beheer, hosting en applicatieondersteuning

Voor de continuïteit, betrouwbaarheid en doorontwikkeling van de getroffenregistratiesystematiek is het noodzakelijk om het **technisch beheer, de hosting en de applicatieondersteuning** structureel te organiseren en te borgen. Gezien het specialistische karakter van het systeem, de specifieke gebruikersgroep en de vereiste beschikbaarheid tijdens incidenten en oefeningen, wordt voorgesteld om deze taken **extern te beleggen**. Daarmee worden deze taken uitgevoerd door een gespecialiseerde leverancier en niet door de organiserende of gebruikende partijen zelf.

Er wordt gestreefd naar een stabiel, veilig en toekomstbestendig systeem dat 24/7 inzetbaar is bij rampen en crises en dat voldoet aan de functionele en technische eisen zoals vastgelegd in het programma van eisen.

Voorgesteld wordt om de verantwoordelijkheid voor de **support, het technisch applicatiebeheer, de instandhouding en de doorontwikkeling** van het getroffenregistratiesysteem uit te laten voeren door een **externe leverancier of ontwikkelaar**. Hieronder vallen ook het beheer van de database en de uitvoering van back-up-gerelateerde activiteiten. Aan de externe leverancier wordt daarnaast gevraagd om de hosting te organiseren, eventueel via een daarin gespecialiseerde hostingpartij.

4.4 Scheiding regie en technisch beheer

Daarnaast wordt voorgesteld om **één landelijke partij verantwoordelijk** te maken **voor de regie** op het getroffenregistratiesysteem. Deze partij ziet erop toe dat het systeem aansluit bij de landelijke werkwijze, de behoeften van de gebruikers en de eisen die gelden binnen het crisisdomein.

De landelijke regiepartij is aanspreekpunt voor de inrichting, kwaliteit, continuïteit en doorontwikkeling van het systeem. Ook ziet deze partij toe op de afspraken met de leverancier, bijvoorbeeld over beschikbaarheid, beveiliging, ondersteuning, updates, rapportages en escalatie bij storingen of crises. Daarmee vormt de landelijke regiepartij de schakel tussen de gebruikers van het systeem, zoals veiligheidsregio's, GHOR, gemeenten en andere betrokken organisaties, en de externe leverancier die verantwoordelijk is voor het technisch beheer, de hosting en de applicatieondersteuning.

Landelijke regie is belangrijk om te voorkomen dat iedere partij het systeem op een eigen manier gaat gebruiken, beheren of doorontwikkelen. Het zorgt voor uniformiteit, duidelijke verantwoordelijkheden en gezamenlijke sturing op de verdere ontwikkeling van het systeem.

Voor de landelijke regie wordt voorgesteld om een partij te kiezen die beschikt over ervaring met vergelijkbare applicaties en die al een bestaande landelijke rol heeft binnen het crisisdomein. Het NIPV vervult op dit moment een dergelijke rol bij de regie op het Landelijk

Crisismanagement Systeem (LCMS). Het LCMS heeft duidelijke raakvlakken met de doelstellingen van het centrale getroffenregistratiesysteem. Daarom ligt het voor de hand om te verkennen of het NIPV ook de regie op dit systeem op zich kan nemen. Eventuele andere landelijke partijen die deze rol zouden kunnen vervullen, zijn de betrokken ministeries van VWS en JenV, of een gemandateerde veiligheidsregio die namens de andere partijen de regierol op zich neemt.

Deze constructie, waarbij de landelijke regie wordt gescheiden van het technisch beheer, biedt duidelijke voordelen. Extern technisch beheer kan zorgen voor professionele ondersteuning, betere beschikbaarheid, betere schaalbaarheid bij incidenten en een hogere mate van continuïteit. Ook kan een gespecialiseerde leverancier processen inrichten voor monitoring, beveiliging, back-up en herstel. Hierdoor kan de landelijke regiepartij zich richten op sturing, kwaliteit, doorontwikkeling en afstemming binnen het crisisdomein, in plaats van op de dagelijkse technische uitvoering.

4.5 SaaS-overeenkomst

Voorgesteld wordt om het getroffenregistratiesysteem af te nemen op basis van een SaaS-overeenkomst. SaaS staat voor *Software as a Service*. Dit betekent dat de applicatie niet lokaal wordt geïnstalleerd of volledig in eigen beheer wordt ontwikkeld, maar via internet beschikbaar wordt gesteld door een leverancier. De leverancier is daarbij verantwoordelijk voor de beschikbaarheid, hosting, technisch beheer, updates, beveiliging en ondersteuning van de applicatie.

Een belangrijk voordeel van een SaaS-overeenkomst is dat gebruik kan worden gemaakt van bestaande technische expertise en infrastructuur van een gespecialiseerde leverancier. Hierdoor kan het systeem professioneel worden beheerd, sneller worden doorontwikkeld en beter worden opgeschaald bij incidenten of crises. Ook kunnen afspraken over beschikbaarheid, responstijden, beveiliging, back-ups, herstelmogelijkheden en ondersteuning duidelijk worden vastgelegd in de overeenkomst.

Tegelijkertijd vraagt een SaaS-overeenkomst om goede contractuele waarborgen. Er moet onder andere aandacht zijn voor privacy en informatiebeveiliging, verwerking van persoonsgegevens, eigenaarschap van data, auditmogelijkheden, continuïteit, exit-afspraken en de overdraagbaarheid van gegevens bij beëindiging van de overeenkomst. Ook moet duidelijk zijn wie opdrachtgever is, wie gebruiker is en wie verantwoordelijk is voor landelijke regie, organisatorisch beheer, leveranciersmanagement en escalatie bij verstoringen.

In dit geval ligt een SaaS-overeenkomst voor de hand, omdat het getroffenregistratiesysteem 24/7 beschikbaar moet zijn, veilig moet functioneren en tijdens rampen en crises snel moet kunnen opschalen. Door te kiezen voor een SaaS-constructie kan gebruik worden gemaakt van een professioneel beheerde applicatie, terwijl de landelijke regiepartij zich vooral kan richten op sturing, kwaliteit, doorontwikkeling en afstemming met de gebruikers binnen het crisisdomein.

4.6 Eigenaarschap en gebruikersovereenkomst

Omdat het getroffenregistratiesysteem naar verwachting als SaaS-oplossing wordt afgenomen, wordt de landelijke regiepartij in beginsel geen eigenaar van de applicatie. Bij een SaaS-oplossing blijft de applicatie in beginsel eigendom van de leverancier of ontwikkelaar. De gebruiker krijgt toegang tot de applicatie, maar wordt daarmee geen eigenaar van de software zelf.

De afspraken met de leverancier worden vastgelegd in een SaaS-overeenkomst. Hierin worden onder andere afspraken gemaakt over het gebruik van de software, hosting, technisch beheer, beschikbaarheid, beveiliging, support, updates, back-ups, herstelmogelijkheden, gegevensverwerking, rapportages en exit-afspraken bij beëindiging van het contract. Bij het maken van deze afspraken zal ook gekeken worden waar de data opgeslagen wordt, zodat deze niet in handen komt van andere partijen/actoren met mogelijk ongewenste intenties, zowel binnen als buiten Nederland.

Indien bijvoorbeeld het NIPV de landelijke regierol op zich neemt, kan het NIPV optreden als landelijke regiepartij en gebruiker van het systeem. Het gebruik van de applicatie wordt dan vastgelegd in een gebruikersovereenkomst. Daarin worden afspraken gemaakt over onder andere toegang tot het systeem, rollen en verantwoordelijkheden, autorisaties, gebruiksregels, gegevensverwerking, ondersteuning, beschikbaarheid, beveiliging en naleving van de gemaakte afspraken.

Deze afbakening is belangrijk om duidelijk onderscheid te maken tussen het eigenaarschap van de applicatie, de contractuele afspraken met de leverancier, de landelijke regie op het systeem, het technisch beheer en het feitelijke gebruik van de applicatie door het NIPV en andere betrokken partijen. Daarmee wordt voorkomen dat onduidelijkheid ontstaat over wie verantwoordelijk is voor de applicatie, de gegevens, het leveranciersmanagement, het dagelijks gebruik van het systeem en de besluitvorming over doorontwikkeling.

4.7 Minimaal benodigde diensten

Voor het getroffenregistratiesysteem is een aantal diensten minimaal noodzakelijk om het systeem betrouwbaar, veilig en toekomstbestendig te kunnen gebruiken. In bijlage 1 is een overzicht opgenomen van de minimaal benodigde diensten.

De dienstverlener moet toegang bieden tot de applicatie via internet (inclusief een fallback scenario), zodat deze gebruikt kan worden op verschillende apparaten, zoals telefoons, tablets en desktop-pc's. Daarbij horen ook het beheer van functionaliteiten, updates, nieuwe releases, bugfixes, configuratiemogelijkheden en gebruikers- en rollenbeheer.

Daarnaast is de dienstverlener verantwoordelijk voor de hosting en technische infrastructuur van het systeem. Dit omvat onder andere de hosting van de applicatie en databases. Een belangrijk onderdeel is de beveiliging van het systeem en de gegevens. De dienstverlener moet zorgen voor adequate beveiligingsmaatregelen, zoals multifactor-

authenticatie en een veilige infrastructuur. Daarbij moet worden voldaan aan relevante wet- en regelgeving en standaarden, waaronder de AVG.

Ook het beheer van data moet zorgvuldig zijn ingericht. Dit betekent dat gegevens veilig worden opgeslagen en beheerd, dat er back-ups en herstelmogelijkheden beschikbaar zijn en dat afspraken worden gemaakt over datatoegankelijkheid, exportmogelijkheden, bewaartermijnen en verwijdering van gegevens.

Verder moet het systeem kunnen koppelen met andere relevante systemen. De dienstverlener moet daarom voorzien in Application Programming Interfaces (API's) of standaardkoppelingen. API's zijn digitale koppelingen waarmee verschillende softwareprogramma's met elkaar kunnen communiceren en gegevens kunnen uitwisselen.

Tot slot zijn goede ondersteuning, servicemanagement en contractuele afspraken noodzakelijk. De dienstverlener moet voorzien in een servicedesk voor incidenten en vragen, een kennisbank en documentatie, duidelijke afspraken over responstijden en beheer van updates en gepland onderhoud. Ook moeten afspraken worden vastgelegd over servicelevels, zoals uptime, performance en responstijden, de verwerkersovereenkomst in het kader van de AVG, audit- en compliance-informatie, transparante tarieven en licentiebeheer.

4.8 Aandachtspunten en conclusies

Tegenover de voordelen van externe uitvoering en een SaaS-constructie staan ook aandachtspunten. Door het beheer van het systeem extern te beleggen, ontstaat afhankelijkheid van één leverancier en mogelijk ook van diens hostingpartij. Dit kan leiden tot minder grip, complexere aansturing en risico's bij storingen, contractbeëindiging of onvoldoende prestaties.

Verder vraagt uitbesteding van een systeem waarin mogelijk gevoelige persoonsgegevens worden verwerkt om strikte eisen op het gebied van privacy, informatiebeveiliging, auditmogelijkheden, toegangsbeheer en continuïteit. Ook is het van belang dat de leverancier voldoende begrip heeft van de specifieke eisen die horen bij crisisbeheersing, waaronder snelle opschaling, piekbelasting tijdens incidenten en het werken met meerdere betrokken organisaties.

Vanwege deze aandachtspunten verdient het aanbeveling om in de aanbesteding extra waarde toe te kennen aan partijen die al bewezen technologie aanbieden voor het gewenste systeem. Daarmee kan het risico worden verkleind dat een volledig nieuwe of onvoldoende beproefde oplossing moet worden ontwikkeld voor een systeem dat juist onder crisissomstandigheden betrouwbaar moet functioneren.

Ondanks deze aandachtspunten is de conclusie dat externe uitvoering van het technisch beheer, de hosting en de applicatieondersteuning, in combinatie met landelijke regie op het systeem, de voorkeur heeft. Deze inrichting biedt de beste waarborgen voor continuïteit, professionaliteit, schaalbaarheid en landelijke uniformiteit. Voorwaarde is wel dat de

governance stevig wordt ingericht en dat in het programma van eisen en de contractuele afspraken helder wordt vastgelegd wie welke verantwoordelijkheden draagt.

Ook moeten eisen worden gesteld aan beschikbaarheid, hersteltermijnen, gegevensbescherming, periodieke tests, rapportages en overdraagbaarheid bij beëindiging van het contract. Dit moet worden opgenomen in het programma van eisen.

De bovenstaande voordelen worden ook door de veiligheidsregio's erkend. Zij geven de voorkeur aan landelijke regie, vergelijkbaar met de wijze waarop dit bij LCMS is ingericht. Dit hebben de experts vanuit Bevolkingszorg aangegeven tijdens de verkenning in fase 1.

5 Beschrijving van Programma van Eisen op hoofdlijnen

Dit hoofdstuk omvat het Programma van Eisen voor het getroffenregistratiesysteem *op hoofdlijnen*. Het beschrijft de minimale functionele, technische en beheersmatige eisen waaraan de toekomstige voorziening moet voldoen. Na goedkeuring van fase 2 kan de (nieuwe) projectgroep samen met de betrokken partijen aan de slag met een gedetailleerde uitwerking.

De eisen zijn thematisch geordend in drie samenhangende delen: 1) het registreren, traceren, matchen en volgen van getroffen, 2) het systeembeheer en de administratieve functies, en 3) het informeren en communiceren met betrokkenen en organisaties. In bijlage 2 staan de verschillende onderdelen in tabelvorm.

Het Programma van Eisen op hoofdlijnen is een eerste inhoudelijk kader voor de verdere ontwikkeling en inrichting van het systeem. Na goedkeuring van het stappenplan voor de volgende fases moet in samenwerking met de stakeholders het Programma van Eisen op detailniveau verder uitgewerkt worden, ter voorbereiding op het aanbestedingstraject. Dat is noodzakelijk, omdat het beoogde systeem niet alleen functionele ondersteuning moet bieden voor registratie, tracing en matching, maar ook eisen stelt aan beveiliging, privacy, toegangsbeheer, continuïteit, koppelingen, support, auditing en opleiding (zie hoofdstuk 'Juridische quickscan'). De aanbestedingsstrategie moet daarom ruimte bieden om deze samenhangende eisen zorgvuldig uit te werken en bij de stakeholders uit te vragen.

5.1 Deel A: Registreren (fysiek, digitaal), traceren en volgen

Het getroffenregistratiesysteem moet voorzien in een eenduidige en betrouwbare registratie van getroffen, verwanten en vermisten (het stellen van een zoekvraag) tijdens rampen en crises. Het systeem ondersteunt verschillende vormen van registratie, waaronder registratie via de frontoffice van SIS, in opvanglocaties, ziekenhuizen, gemeenten, incidentlocaties en via online zelfregistratie. Hiermee wordt geborgd dat informatie vanuit meerdere bronnen op een gestructureerde manier kan worden vastgelegd en verwerkt.

Een belangrijk uitgangspunt is dat persoonsdossiers ook kunnen worden aangemaakt wanneer nog niet alle gegevens over een persoon beschikbaar zijn. In crisissituaties is informatie vaak onvolledig of onzeker. Het systeem moet daarom flexibel genoeg zijn om gegevens later aan te vullen, te wijzigen of te koppelen. Daarnaast moet het mogelijk zijn om lijsten, zoals passagierslijsten of registraties vanuit opvanglocaties, in te laden in het systeem.

Het systeem moet ook de mogelijkheid bieden om verschillende registratiepunten in te richten, zoals een callcenter, opvanglocatie, ziekenhuis, lokaal steunpunt of andere incident-specifieke locatie. Deze registratiepunten moeten per incident kunnen worden toegevoegd,

aangepast of via een koppeling worden ingeladen. Daarbij moet de actuele locatie van een getroffenene kunnen worden vastgelegd en automatisch worden bijgewerkt wanneer iemand op een andere locatie opnieuw wordt ontvangen.

Voor burgers moet het mogelijk zijn om via online 'registratiemodules' informatie aan te leveren of te zoeken. Dit kan gaan om zelfregistratie door getroffenen, met daaraan bijvoorbeeld toegevoegd de melding 'ik ben veilig', of om zoekvragen van verwanten die op zoek zijn naar een naaste. Bij zelfregistratie kan een unieke code, QR-code of barcode worden aangemaakt door het systeem, zodat personen en dossiers op een betrouwbare manier kunnen worden herkend en gekoppeld. Indien een persoon een zoekvraag indient ontvangt de frontoffice SIS deze digitale informatie die aan de slag gaat met het verwerken van de zoekvraag. Deze registratiemodules moeten in te passen zijn in een website die fungeert als Informatie- en Verwijscentrum (IVC) / Eénloketsfunctie, waar ook informatie over het incident te vinden is.

Een centrale functie van het systeem is het kunnen koppelen en matchen van informatie. Gegevens van verwanten, vermisten, getroffenen en niet-zelfredzame slachtoffers moeten met elkaar in verband kunnen worden gebracht.

5.2 Deel B: Systeembeheer en administratieve functies

Naast de functionele registratie- en matchingsmogelijkheden moet het getroffenenenregistratiesysteem beschikken over goede beheer- en administratieve functies. Deze functies zijn noodzakelijk om het systeem veilig, controleerbaar en betrouwbaar te kunnen gebruiken tijdens rampen, crises, oefeningen en reguliere voorbereidingsactiviteiten.

Een belangrijk onderdeel hiervan is het kunnen aanmaken, beheren, bewaren en verwijderen van incidenten of cases. Per incident moet het mogelijk zijn om de juiste instellingen, registratiepunten, gebruikers en gegevensstromen in te richten. Ook moet het systeem ondersteuning bieden bij het groeperen van gegevens, bijvoorbeeld door het gebruik van groepscode voor verwanten, vermisten of andere betrokken groepen. Naast deze functionaliteiten moet het voor bepaalde functieprofielen ook mogelijk zijn om persoonsdossiers te corrigeren, verwijderen of onzichtbaar (bv overledenen) te maken voor anderen. Daarnaast moet het systeem beschikken over zorgvuldig identiteits- en toegangsbeheer. Dit betekent dat accounts voor gebruikers kunnen worden aangemaakt, gewijzigd en verwijderd en dat gebruikers op basis van rollen en rechten toegang krijgen tot de specifieke onderdelen van het systeem die zij nodig hebben voor het uitvoeren van hun taak. Daarbij moet het mogelijk zijn dat één functieprofiel meerdere rollen heeft. Activiteiten van gebruikers moeten worden gelogd, zodat inzichtelijk is wie welke handelingen heeft uitgevoerd.

Auditing en logging zijn belangrijke randvoorwaarden. Het systeem moet voorzien in centrale auditing voor zowel het getroffenenenregistratiesysteem als het burgerportaal. Daarmee kan achteraf worden gecontroleerd welke gegevens zijn geraadpleegd,

gewijzigd of gedeeld. Dit is van belang voor verantwoording, informatiebeveiliging, privacy en naleving van wet- en regelgeving.

Ook moeten de technische eisen helder zijn vastgelegd. Het systeem moet inzicht geven in de wijze waarop bijvoorbeeld de architectuur, hosting, beveiliging, identiteit- en toegangsbeheer zijn geregeld. Daarnaast moeten afspraken worden gemaakt over integraties, API's, updates, capaciteit, monitoring, privacy, etc.

Tot slot moet het systeem beschikken over een aparte oefen- of opleidingsomgeving. Deze omgeving moet gebruikt kunnen worden voor trainingen, opleidingen en oefeningen, zonder dat dit invloed heeft op de productieomgeving of op echte persoonsgegevens. Hiermee kunnen gebruikers ervaring opdoen met het systeem en kunnen processen periodiek worden getest en verbeterd.

5.3 Deel C: Informeren en communiceren

Het getroffenregistratiesysteem moet ook ondersteunen bij het informeren en communiceren tijdens een incident. Tijdens rampen en crises is er grote behoefte aan actuele, betrouwbare en overzichtelijke informatie. Het systeem moet daarom informatie kunnen bundelen en presenteren in rapportages, dashboards en lijsten die aansluiten bij de rol en informatiebehoefte van de gebruiker.

Een belangrijk onderdeel is het kunnen genereren van rapporten (exporteerbare word documenten) per incident. Afhankelijk van de functie en autorisatie van de gebruiker moet het systeem verschillende rapportages kunnen bieden, zoals rapportages over triage en pre-triage aantallen, overzichten van aantallen getroffen en verwanten (zowel totaallijsten, als ook per registratiepunt), en overzichten met (openstaande) zoekvragen. Ook moet het mogelijk zijn om rapportages te sorteren of te filteren op bijvoorbeeld nationaliteit, locatie, registratiepunt of groepscode.

Daarnaast moet het systeem beschikken over dashboards die een actueel totaalbeeld geven van het incident. Deze dashboards ondersteunen de informatievoorziening richting bijvoorbeeld CoPI en ROT. Het dashboard moet inzicht geven in relevante aantallen en ontwikkelingen, zoals aantallen en triageclassificatie van slachtoffers, verwanten, getuigen, telefoontjes (zoekvragen), personen per locatie en personen die de hulpverlening hebben verlaten of onderweg naar huis zijn. De exacte inrichting van het dashboard moet in samenspraak met de stakeholders verder worden uitgewerkt.

Ook moet het systeem verschillende lijsten kunnen genereren, met daarbij passende toegangsrechten. Hierbij gaat het onder andere om lijsten van vermisten gekoppeld aan verwanten, slachtofferlijsten, vermistenlijsten, dodenlijsten en lijsten met (zelf)geregistreerde getroffen ten behoeve van de nafase. Daarnaast moet het systeem kunnen ondersteunen bij het verstrekken van informatie aan verwanten, zodat zij duidelijkheid krijgen over het verloop van het proces en de vervolgstappen met betrekking tot hun zoekvraag.

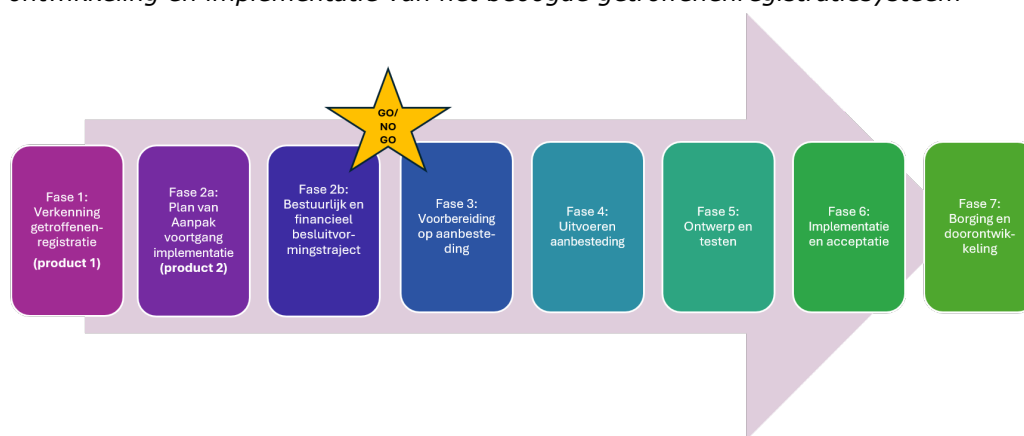
Deze functies dragen bij aan een eenduidig informatiebeeld, betere besluitvorming en zorgvuldige communicatie met betrokken organisaties en crisisstructuren. Daarbij is het van belang dat alleen geautoriseerde gebruikers toegang hebben tot de informatie die zij nodig hebben voor hun taak.

Deel B - Stappenplan en aanbevelingen

6 Stappenplan voor fase 3 en verder

In dit hoofdstuk staan de verschillende stappen van de achtereenvolgende fases in het proces beschreven om te komen tot een functionerend centraal getroffenregistratiesysteem. In onderstaand figuur zijn de verschillende fases, van verkenning tot implementatie en borging onderscheiden.

Figuur 6.1 Fases in het proces van verkenning, besluitvorming, aanschaf, ontwikkeling en implementatie van het beoogde getroffenregistratiesysteem



6.1 Fase 3: Voorbereiding op aanbesteding (3-6 maanden)

Voordat de aanbesteding kan starten zal het Programma van Eisen uitgewerkt moeten worden. In fase 2a is hiervoor een globale opzet gemaakt, in fase 3 zal de detaillering hiervan plaatsvinden. Hierin wordt per onderdeel aangegeven wat de uit te voeren acties en de op te leveren producten zijn. De informatie is gehaald uit de openbare informatie over Europese aanbestedingen. Gezien de complexiteit van de opgave en de grootte van het stakeholderveld is de verwachting dat deze voorbereidende fase eerder in de buurt van een 6 maanden zal uitkomen.

Randvoorwaarden om te starten met fase 3 zijn het commitment van de betrokken partijen en de toezegging van de financiering. Hierover is, in geval van doorgang, een positief besluit genomen in fase 2b.

In fase 3 gaat het vooral om nog gedetailleerder begrijpen wat de verschillende stakeholders nodig hebben. Wat moet de nieuwe applicatie exact kunnen? In de verkenning en in het plan van aanpak zijn hier de eerste stappen al voor gezet, in deze fase zal de aanscherping volgen op basis van consultatie van de stakeholders vanuit de verschillende deelprojecten/processen.

In deze periode wordt tevens een markconsultatie gehouden: leveranciers worden uitgenodigd om mee te denken. Ze vertellen over trends, over de mogelijkheden van SaaS, security-eisen en mogelijke koppelingen. Vaak komt in deze fase al naar voren dat sommige wensen

eenvoudiger kunnen dan gedacht — of juist ingewikkelder zijn. Dit kan dan meegenomen worden in het bestek.

Parallel werkt het projectteam aan de inkoopstrategie: wat gaan we precies vragen, hoe gaan we beoordelen, welke eisen zijn “knock-outs” en wat laten we open voor innovatie? Tegelijkertijd worden functionele eisen geschreven, juridische modellen besproken en intern de budgetten geborgd. Aan het eind van deze fase ligt er een duidelijk pakket met documenten die nodig zijn voor de aanbesteding.

De aanbestedende organisatie is verantwoordelijk voor het aanbestedingsproces. In de voorbereidingen wordt zorgvuldig consensus gezocht met het veld.

Producten/deliverables die in deze fase verder opgeleverd worden:

- Aanbestedingsdocumenten
 - o Beschrijvend document (bestek):
 - Omschrijving van de opdracht,
 - Gewenst kwaliteitsniveau,
 - De administratieve voorwaarden,
 - De selectiecriteria,
 - De gunningscriteria,
 - Programma van Eisen: eisen aan het systeem (functionele en non-functionele eisen/wensen, technische eisen, eisen voor de inschrijver, implementatieplan),
 - o Contractvoorwaarden/overeenkomst,
- Nota van Inlichtingen (document waarin vragen van inschrijvers worden beantwoord en aanpassingen in de stukken worden gecommuniceerd).
- Projectplan en planning aanbesteding
- Marktconsultatieverslag (optioneel)
- Inkoopstrategie / aanbestedingsstrategie

Doelen in deze fase:

- Markt begrijpen (bv. SaaS vs maatwerk)
- Definitieve aanbestedingsdocumenten

6.2 **Fase 4: Uitvoering van aanbesteding (5-10 maanden)**

Het uitvoeren van een aanbesteding bestaat uit een aantal achtereenvolgende stappen, die hieronder in chronologische volgorde worden beschreven (zie ook tabel in hoofdstuk 6.6).

Figuur 6.2 De verschillende stappen van de aanbesteding in chronologische volgorde



6.2.1 *Publicatie (1-2 weken)*

Op een afgesproken dag gaat de aanbesteding de lucht in. De publicatie verschijnt op TenderNed en automatisch ook op TED, waardoor heel Europa het kan zien. Vanaf dat moment gaan leveranciers de stukken downloaden, de eisen bestuderen en bepalen of ze willen inschrijven. Voor de projectorganisatie breekt een relatief stille periode aan, tot het moment dat de vragen binnenkomen.

Producten/deliverables:

- Officiële aankondiging (bekendmaking)
- Aanbestedingsstukken (PvE, Nota van Inlichtingen, deadlines, planning)
- Conceptovereenkomst inclusief SLA (*service level agreement*)

6.2.2 *Vragenronde(s) – Nota van Inlichtingen (4-8 weken)*

Leveranciers willen verduidelijking en kunnen in deze fase vragen stellen. De organisatie beantwoordt de vragen zorgvuldig, vaak met multidisciplinaire teams (juridisch, technisch, functioneel, privacy). Het resultaat verschijnt in een of meerdere Nota's van Inlichtingen. Daarin worden enkele eisen soms aangescherpt of juist versoepeld. De stukken worden door de Nota van Inlichtingen formeel bindend. De markt weet nu precies waar aan voldaan moet worden.

Producten/deliverables:

- Nota('s) van Inlichtingen met officiële antwoorden
- Aangepaste aanbestedingsstukken (indien nodig)

Aantal rondes: meestal 1–2, maar bij softwareaanbestedingen vaker 2–3.

6.2.3 *Indienen van inschrijvingen (6-10 weken)*

Leveranciers leveren hun offerte(s) in conform de eisen en criteria.

Producten/deliverables van inschrijvers:

- Volledige offerte met prijsblad
- Bewijsstukken (UHD, GVA, referentieprojecten)
- Plan van aanpak
- Technische documentatie (architectuur, beveiliging, integraties)
- Concept-DPIA of security assessment (soms verplicht).

6.2.4 *Beoordeling van inschrijvingen (6-12 weken)*

Elke offerte wordt onafhankelijk gelezen en beoordeeld. Bij IT-projecten kijken vaak verschillende disciplines mee, zoals inkoop, functioneel beheer, security, privacy en bedrijfsvoering. Er wordt gescoord op kwaliteit en op prijs. Soms verrassen leveranciers met slimme oplossingen, soms blijkt dat een veelgevraagde functionaliteit toch niet

geleverd kan worden. Als alle scores binnen zijn, wordt een consensusvergadering gehouden met de personen die de offertes individueel beoordeeld hebben. Daar worden de individuele beoordelingen besproken en komt een eindscore tot stand. Dat leidt tot een gunningsadvies.

De aanbestedende organisatie beoordeelt alle inschrijvingen op de uitsluitings- & geschiktheidseisen, daarna de kwalitatieve criteria en de prijs.

Veelgebruikte gunningsmethodes:

- Beste Prijs Kwaliteit Verhouding (BPKV, gebruikelijk bij applicaties)
- Laagste prijs (zelden bij IT-projecten)

Producten/deliverables:

- Beoordelingsrapport
- Interne besluitvorming (gunningsadvies)

6.2.5 *Voornemen tot gunning (20 dagen)*

Nadat de winnaar is gekozen, krijgen álle inschrijvers bericht over wie gewonnen heeft, waarom en hoe zij zelf gescoord hebben.

Daarmee gaat de standstill-periode (Alcatel-termijn) van 20 dagen in. Leveranciers die het er niet mee eens zijn, kunnen in deze 20 dagen bezwaar maken. Vaak gebeurt er niets, soms volgt nog een juridische discussie. Als de periode zonder problemen verloopt, kan het contract definitief worden gesloten.

Producten/deliverables:

- Voornemen tot gunning
- Afwijzingsbrieven
- Verslag van de gunningsbeslissing.

6.2.6 *Contractering (2-8 weken)*

Na de standstill-periode worden de contract(en) afgerond. Indien nodig wordt de planning aangescherpt of worden mijlpalen verder geconcretiseerd. Na het moment van contractering gaat het project over naar de volgende stap; het ontwerp en testen van het beoogd systeem (fase 5).

Producten/deliverables:

- Ondertekende overeenkomst
- SLA
- Beveiligingsafspraken
- Implementatieplanning
- Eventueel: Data Protection Impact Assessment (DPIA) finale versie
- Escrow-regeling (optioneel)

6.3 Fase 5: Ontwerpen en testen van beoogd systeem (5 - 10 maanden)

In deze fase wordt het beoogde systeem daadwerkelijk vormgegeven en voorbereid op gebruik. In deze periode werkt de leverancier samen met het projectteam aan het uitwerken van het ontwerp, het realiseren van technische koppelingen en het testen van de werking van het systeem. Deze fase bestaat uit verschillende stappen, met verschillende producten.

In deze fase zal ook een scholingsplan met bijbehorende middelen ontwikkeld worden voor het opleiden van de gebruikers van het systeem. Net als een communicatieplan om gebruikers, de partijen in het crisismanagement veld en de maatschappij te informeren over de komst van het registratiesysteem. Hiermee wordt de basis gelegd voor een succesvolle implementatie en uiteindelijke ingebruikname van het systeem.

De duur van deze fase is sterk afhankelijk van de resultaten van de aanbesteding. Als een gecontracteerde leverancier van nul moet beginnen met het ontwerp van een systeem, zal dit meer tijd in beslag nemen dan wanneer een leverancier slechts aanpassingen hoeft te doen op een bestaande technologie. Dit maakt het schatten van een tijdsbesteding voor deze fase lastig. De ontwikkeling van het Belgische systeem heeft meerdere jaren gekost, omdat er toentertijd geen andere bewezen technologie beschikbaar was en tussentijds nog gewisseld is van leverancier.

Randvoorwaardelijke acties en producten (deliverables):

- Projectplan van leverancier
- Ontwerpdocumenten
- Koppelingen en integraties
- Acceptatietesten
- MVP (minimum viable product, de eerste versie van een product of dienst die net genoeg functies bevat om bruikbaar te zijn, dus geen nice-to-haves)
- DPIA uitvoeren
- Scholingsplan voor opleiden gebruikers
- Communicatieplan

6.4 Fase 6: Acceptatie en implementatie van beoogd systeem (3 - 6 maanden)

In deze fase wordt het ontwikkelde systeem daadwerkelijk in gebruik genomen en getest in de praktijk. Het doel is om te controleren of het systeem goed functioneert en voldoet aan alle gestelde eisen. Door middel van een pilot in (een) geselecteerde veiligheidsregio('s) wordt ervaring opgedaan en kunnen eventuele aanpassingen of verbeterpunten worden geïdentificeerd.

Daarnaast ligt de focus op het voorbereiden van de betrokken organisaties op het gebruik van het systeem. Dit gebeurt onder andere door het verzorgen van opleidingen en trainingen (de uitvoering van het scholingsplan). Daarnaast worden in deze fase samenwerkings- en verwerkersovereenkomsten opgesteld. Naast de

samenwerkingsovereenkomsten is het ook van belang dat er een beschrijving komt van de werkprocessen in de praktijk. Wie doet er nu precies wat? Mogelijk moeten bestaande werkafspraken iets aangepast worden.

Verder wordt er in deze fase een go-live checklist ontwikkeld en uitgevoerd. Ook wordt er een OTO-programma (Opleiden, Trainen en Oefenen) ingericht en uitgerold om het gebruik van het systeem te borgen na ingebruikname.

Aan het einde van deze fase wordt het systeem officieel in gebruik genomen en overgedragen aan de beheerorganisatie, inclusief nazorg om een soepele overgang te garanderen.

Randvoorwaardelijke acties en producten (deliverables):

- Pilot draaien in een/meerdere nader te bepalen veiligheidsregio('s)
- Go-live checklist
- OTO-programma opstellen en uitrollen
- Opleidingen en trainingen (train-de-trainer)
- Samenwerkingsovereenkomsten opstellen
- Verwerkersovereenkomsten opstellen en beschrijven/aanpassen van werkprocessen in de praktijk
- Nazorg en overdracht naar beheer

6.5 Fase 7: Borging en doorontwikkeling beoogd systeem

In deze fase ligt de focus op het duurzaam borgen en verder ontwikkelen van het systeem. Het doel is om ervoor te zorgen dat het systeem ook op de lange termijn effectief, veilig en actueel blijft. Door middel van beheerafspraken, evaluaties en een doorontwikkelagenda wordt continu gewerkt aan verbetering. Daarnaast wordt het gebruik van het systeem geborgd door middel van handleidingen, trainingen en eventuele aanpassingen in de werkafspraken.

Randvoorwaardelijke acties en producten (deliverables):

- Organisatieplan
- Beheer- en onderhoudsplan
- Service Level Agreements (SLA's)
- Handleiding en werkinstructies voor gebruikers
- Uitvoeren van OTO-programma (doorlopend)
- Doorontwikkelagenda / roadmap
- Continuïteitsplan/ fall back plan (bij storingen/crises)

6.6 Tijdslijn samengevat

Tabel 6.1 Samenvatting van de geschatte tijdslijn voor aanschaf, ontwerp en implementatie van een centraal getroffenregistratiesysteem

Onderdeel	Duur	Belangrijkste deliverables
1. Voorbereiding aanbesteding	3–6 maanden	Strategie, eisen, PvE
2. Publicatie	1–2 weken	Aankondiging, stukken
3. Vragenrondes	4–8 weken	Nota's van Inlichtingen
4. Inschrijvingen	6–10 weken	Offertes, technische info
5. Beoordeling	6–12 weken	Beoordelingsrapport
6. Standstill	20 dagen	Voornemen gunning
7. Contractering	2–8 weken	Contract + SLA
8. Ontwerp, testen en implementatie (fase 5 en 6)	8–16 maanden	Implementatieproducten
Totaal	Ca. 31 maanden	

7 Conclusies, bestuurlijke besluitvorming en aanbevelingen

7.1 Conclusies

De uitkomsten van fase 2a laten zien dat een centraal getroffenregistratiesysteem zowel technisch, juridisch als organisatorisch haalbaar is en een duidelijke maatschappelijke meerwaarde heeft.

7.2 Bestuurlijke besluitvorming

Voor succesvolle realisatie is het essentieel dat in fase 2b bestuurlijk commitment wordt verkregen en afspraken worden gemaakt over de scope van de opdracht, financiering, governance en opdrachtgever- en opdrachtnemerschap. Bij positief besluit tot voortgang, kan in fase 3 worden gestart met de voorbereiding op de aanbesteding.

De informatie die verzameld is in fase 2a is nodig om in fase 2b het besluitvormingstraject te voeden. Gedurende het besluitvormingstraject wordt een, bestuurlijk akkoord gevraagd op tenminste de volgende zaken:

- Het inhoudelijke voorstel voor een centraal getroffenregistratiesysteem bij rampen, crises en grootschalige incidenten. Men committeert zich aan het gebruik van dit systeem, omdat dit is wat men wil en er zullen geen alternatieve systemen gebruikt worden voor de getroffenregistratie.
- Het voorstel voor beheer, hosting en regie/coördinatie op de applicatie, zoals beschreven in deze rapportage.
- Het financieringsvoorstel, opgesteld door de veiligheidsregio's in afstemming met de ministeries van JenV en VWS en andere stakeholders, met daarin een duidelijke verantwoordelijkheidsverdeling over de verschillende betrokken stakeholders. De relevante stakeholders committeren zich gezamenlijk aan de verantwoordelijkheid voor zowel operationele inzet als financiële instandhouding (de structurele kosten).
- De ondersteunende en faciliterende rol van de ministeries van Justitie en Veiligheid en Volksgezondheid, Welzijn en Sport, gericht op het versterken van bestuurlijke afstemming en het creëren van randvoorwaarden voor het vervolgtraject.
- De betrokken stakeholders stellen uren beschikbaar om deel te nemen in de projectorganisatie vanaf fase 3 en verder. Daarnaast stellen zij uren ter beschikking om hun eigen personeel te scholen in het gebruik van de applicatie en deze kennis ook te onderhouden door middel van borging in de OTO-activiteiten in de regio's.

Voor een succesvolle implementatie en gebruik van het systeem – en dus de voortgang naar fase 3 – is het nodig dat de 'kritieke massa' akkoord gaat met de bovengenoemde besluitpunten. Om deze kritieke massa te behalen is het noodzakelijk dat ten minste een meerderheid van de veiligheidsregio's en gemeenten (in het kader van bevolkingszorg en publieke gezondheidszorg) akkoord gaan, of de intentie uitspreken om op (korte) termijn alsnog aan te zullen sluiten.

Daarnaast zullen ook de meerderheid van de ambulancediensten mee moeten doen, en moet er – middels een besluit vanuit de leden – door AZN een centrale koppeling worden gemaakt met de ritformulieren en vooraankondigingen van de ambulancediensten. Overige partijen kunnen middels een groeimodel eventueel later aansluiten.

7.3 Aanbevelingen ten behoeve van het beoogde systeem

In de vervolgfases moeten er nog een aantal belangrijke besluiten genomen worden over de inrichting van de applicatie en de koppeling met andere systemen. Hierover doen we een aantal aanbevelingen.

Het verdient de aanbeveling om de zelfregistratiemodule en de module voor het registreren van zoekvragen in te bouwen op een publiekswebsite die als centraal **Informatie- en Verwijscentrum** (IVC) kan dienen. In het kader van de psychosociale ondersteuning aan getroffen en is het wenselijk om alle relevante informatie en hulpvragen te kunnen vinden/stellen op één centrale plek (ARQ Nationaal Psychotraumacentrum, 2023). Zo voorkomen we dat mensen van het kastje naar de muur worden gestuurd of niet weten waar ze met hun (informatie)vraag terecht kunnen. Er zijn verschillende mogelijkheden als het aankomt op websites die dienst zouden kunnen doen als Informatie- en Verwijscentrum. Slachtofferhulp Nederland heeft een online Informatie- en Adviescentrum (IAC), een website die ze binnen 1,5 uur online kunnen zetten, met informatie over de gebeurtenis, verwijzingen naar diverse hulpverleners en een mogelijkheid voor lotgenoten contact. Dit IAC is inmiddels bij verschillende rampen en incidenten actief geweest, zoals bij de vliegtuigramp MH17 en het treinongeluk in Voorschoten. De Rijksoverheid (het Nationaal Kernteam Crisiscommunicatie) beheert de website crisis.nl, waarop mogelijk ook koppelingen gemaakt kunnen worden met de online zelfregistratiemodule vanuit het beoogde centrale getroffen en registratiesysteem. Beide opties hebben voor- en nadelen, en een verdere verkenning van kosten en haalbaarheid moet plaats vinden alvorens hier op bestuurlijk niveau een besluit over genomen kan worden.

Naast de online zelfregistratie en de online registratie van zoekvragen in het daadwerkelijke systeem, is het wenselijk om ook een mogelijkheid te bieden voor mensen om zichzelf **veilig te melden** aan de samenleving, en te kunnen zoeken naar anderen die zichzelf veilig hebben gemeld (eventueel met bericht hierbij). Deze informatiestromen moeten, vanuit privacyoverwegingen, gescheiden blijven met de registratiegegevens in het daadwerkelijke systeem. Het Rode Kruis biedt momenteel de 'Ikbenveilig'-applicatie (in het kader van hun taak op het gebied van 'Restoring Family Links') die deze functie vervult. Het is wenselijk om deze functionaliteiten te **integreren in 1 systeem** (dual use) en daarmee de functionaliteit die het Rode Kruis biedt over te nemen. Momenteel wordt de 'Ikbenveilig' applicatie geëvalueerd door het Rode Kruis. De besluitvorming hierover zal de resultaten van deze evaluatie ook mee moeten nemen.

In de verkenning zijn nog een aantal andere mogelijke koppelingen naar voren gekomen, zoals die met de Elektronisch Patiëntendossier (EPD's) binnen de ziekenhuizen. Gezien de complexiteit (het gaat hier om medische dossiers van patiënten), de nog onduidelijke kosten van de opgave en de mogelijk beperkte extra opbrengst (het gaat meestal om een klein deel van de totale populatie getroffen) ten opzichte van de koppeling met de ambulancesystemen, raden we aan om de prioriteit te leggen bij het maken van de koppeling met de ambulancesystemen en **later te kijken naar de eventuele koppeling met de verscheidene ziekenhuissystemen**. Ziekenhuizen leveren nu ook al slachtofferinformatie aan de GHOR in het kader van verwantencontact. Ook als de ziekenhuizen deze informatie handmatig zouden registreren in het beoogde centraal getroffenregistratiesysteem betekent dit een efficiëntieslag ten opzichte van de huidige handelingen.

Literatuur

ARQ Nationaal Psychotraumacentrum. (2023). Multidisciplinaire richtlijn Psychosociaal crisismanagement – ondersteuning en zorg bij rampen en crises. https://arq.org/sites/default/files/2023-06/Multidisciplinaire%20Richtlijn%20Psychosociaal%20Crisismanagement_0.pdf

Gersons, B. P., Smid, G. E., Smit, A. S., Kazlauskas, E., & McFarlane, A. (2020). Can a 'second disaster' during and after the COVID-19 pandemic be mitigated?. *European journal of psychotraumatology*, 11(1), 1815283. <https://www.tandfonline.com/doi/pdf/10.1080/20008198.2020.1815283>

Lock, S., Rubin, G. J., Murray, V., Rogers, M. B., Amlôt, R., & Williams, R. (2012). Secondary stressors and extreme events and disasters: a systematic review of primary research from 2010-2011. *PLoS currents*, 4. <https://pmc.ncbi.nlm.nih.gov/articles/PMC3492002/>

Nederlands Instituut Publieke Veiligheid. (2025, 13 mei). De echte pijn ligt later: de ramp na de ramp - Nederlands Instituut Publieke Veiligheid. Geraadpleegd op 15 april 2026, via <https://nipv.nl/verhalen/de-echte-pijn-ligt-later-de-ramp-na-de-ramp/>

Rooze, M.W. Ruyter, A.M. de, Koopmans A.J.M. (2009). *Modelplan Nafase*. Vormkracht, Odijk & Graphic Support B.V. Deventer. <https://arq.org/sites/default/files/2023-11/Modelplan%20Nafase.pdf>

Verklarende woordenlijst

Lijst met begrippen die in de rapportage worden gehanteerd met de bijbehorende uitleg.

Begrip	Uitleg
Aanbestedingsstrategie	De aanpak voor het inkopen en contracteren van het systeem, inclusief afspraken over implementatie, beheer en doorontwikkeling.
Auditing	Het vastleggen en controleren van handelingen in het systeem, zoals het inzien, toevoegen, wijzigen of delen van gegevens.
Crisis (en incidenten)	In de Wet Veiligheidsregio (Wvr) wordt een crisis als volgt gedefinieerd: 'een situatie waarin een vitaal belang van de samenleving is aangetast of dreigt te worden aangetast'. Bij incidenten worden veelal ingrijpende gebeurtenissen bedoeld die in omvang (veel) kleiner zijn, zoals treinongevallen of een brand waarbij mensen of dieren om het leven komen.
Getroffene	Een persoon die de (potentieel ingrijpende) gebeurtenis heeft ondervonden, er getuige van is geweest of ermee is geconfronteerd in materiële of niet-materiële zin, ongeacht of deze persoon gewond, niet-gewond of overleden is. Onder deze groep vallen bijvoorbeeld de zwaargewonden, nabestaanden van overleden getroffenen, de niet-gewonde ooggetuigen die op termijn psychische klachten ontwikkelen en de personen waarvan het eigen huis onbewoonbaar is verklaard of op andere manier economisch getroffen zijn door een ramp of crisis.
Geneeskundige hulpverleningsorganisatie in de regio (GHOR)	De GHOR is een onderdeel van de Veiligheidsregio, dat tijdens een crisis de geneeskundige hulpverlening coördineert.
Gezondheidsonderzoek bij rampen (GOR)	Wettelijke taak voor de gemeente om de gezondheidstoestand van mensen die getroffen zijn door een ramp of crisis in kaart te brengen.
Herstelzorg	De ondersteuning en acties die het brede herstelproces van de fysieke omgeving en samenleving ondersteunt. Bv. herstelwerkzaamheden aan woning e.d.
Informatie- en Verwijscentrum (IVC)	Digitaal loket dat mensen voorziet van betrouwbare informatie over een specifiek onderwerp en hen als nodig doorverwijst naar verschillende soorten hulp, - zorg- en dienstverleners.
Koppelingen	Technische verbindingen tussen het getroffenregistratiesysteem en andere relevante informatiesystemen voor het veilig uitwisselen van gegevens.
Matching	Het koppelen van gegevens of zoekvragen aan de juiste getroffene, bijvoorbeeld voor het informeren van verwanten.
Nazorg	Het geheel aan georganiseerde psychosociale ondersteuning en zorg die tijdens en/of na een incident, ramp of crisis wordt geboden aan getroffenen en nabestaanden, met als doel om de impact van de gebeurtenis zo veel als mogelijk te beperken.

Begrip	Uitleg
Ramp	In de Wet veiligheidsregio (Wvr) wordt een ramp als volgt gedefinieerd: 'een zwaar ongeval of andere gebeurtenis waarbij het leven en de gezondheid van veel personen, het milieu of grote materiele belangen in ernstige mate zijn geschaad of worden bedreigd en waarbij een gecoördineerde inzet van diensten of organisaties van verschillende disciplines is vereist om de dreiging weg te nemen of de schadelijke gevolgen te beperken'.
Regionaal Operationeel Team (ROT)	Dit is een (multi) tactisch operationeel team, dat de effecten van een crisis in kaart brengt en oplost, de burgemeester adviseert.
Registratie	Het vastleggen en actualiseren van noodzakelijke gegevens over getroffen en. Dit kunnen bijvoorbeeld persoonsgegevens, contactgegevens, de verblijfplaats of opvanglocatie en de behoefte aan ondersteuning zijn.
Slachtoffer	Een gewonde niet-zelfredzame, of overleden getroffene
Slachtoffergegevens	Tot individuen herleidbare (persoons)gegevens van niet-zelfredzame slachtoffers die worden verzameld ten behoeve van het kunnen informeren van verwanten tijdens een incident, ramp of crisis.
Software as a Service (Saas) vergoeding	Een periodieke bijdrage voor gebruik van de software en bijbehorende ondersteuning in plaats van eenmalige aanschafkosten.
Support	De functionele en technische ondersteuning van gebruikers en beheerders bij het gebruik van het systeem.
Toegangsbeheer	Het beheren van gebruikersrechten en autorisaties, zodat gebruikers alleen toegang hebben tot gegevens en functies die zij voor hun taak nodig hebben.
Tracing	Het volgen of achterhalen van de status en indien noodzakelijk, de verblijfplaats van getroffen en gedurende een incident of crisis.
Veiligheidsregio	Een veiligheidsregio is een samenwerkingsverband van gemeenten in een bepaald gebied in Nederland, verantwoordelijk voor brandweezorg, rampenbestrijding, crisisbeheersing en geneeskundige hulpverlening, met als doel de veiligheid en zelfredzaamheid van inwoners te vergroten. Nederland is verdeeld in 25 veiligheidsregio's.
Vermiste	Een mogelijk betrokken getroffene waarnaar gezocht wordt en waarvan niet bekend is waar en in welke toestand deze zich bevindt.
Verwant	Een persoon welke een relatie heeft tot een getroffene en zelf niet betrokken is bij het incident. Het gaat hier bijvoorbeeld om een iemand met een familiale relatie of, in afwezigheid van een familiale relatie, een naaste eerste contactpersoon.

Afkortingenlijst

Lijst met afkortingen die gebruikt worden in de rapportage

Afkorting	Betekenis
API	Application Programming Interfaces
AVG	Algemene Verordening Gegevensbescherming
AZN	Ambulancezorg Nederland
BIO	Baseline Informatiebeveiliging Overheid
BPKV	Beste prijs-kwaliteitsverhouding
BITS-(systeem)	Belgium Incident Tracking System
BZ	Bevolkingszorg
CoPI	Commando Plaats Incident
DPA	Data Processing Agreement
DPIA	Data Protection Impact Assessment
EPD	Elektronisch Patiëntendossier
FTE	Fulltime Equivalent
GGD	Gemeentelijke/Gemeenschappelijke Gezondheidsdienst
GGZ	Geestelijke Gezondheidszorg
GHOR	Geneeskundige Hulpverleningsorganisatie in de Regio
GOR	Gezondheidsonderzoek bij rampen en crises
GVA	Gedragsverklaring Aanbesteden
GZ	Gezondheidszorg
IAC	Informatie- en adviescentrum (van Slachtofferhulp Nederland)
IAM	Identity and Access Management
IDS	Informatie- en dataservices
IT	Informatietechnologie
IVC	Informatie- en Verwijscentrum
JenV	(Ministerie van) Justitie en Veiligheid
LCMS	Landelijk Crisismanagementsysteem
MFA	Multi-Factor Authenticatie
NIPV	Nederlands Instituut Publieke Veiligheid
OTAP	Ontwikkeling, Test, Acceptatie en Productie
OTO	Opleiden, Trainen en Oefenen
OvD-G	Officier van Dienst Geneeskundig
PSH	Psychosociale Hulpverlening
PvE	Programma van Eisen
RBAC	Role-Based Access Control
ROT	Regionaal Operationeel Team
RPO	Recovery Point Objective
RTO	Recovery Time Objective
SaaS	Software as a Service
SLA	Service Level Agreement
SIEM	Security Information and Event Management
SIS	Slachtoffer Informatie Systematiek
SSO	Single Sign-On
T (1-3)	Triageclassificatie (1-3)
VWS	(Ministerie van) Volksgezondheid, Welzijn en Sport
WGBO	Wet op de geneeskundige behandelingsovereenkomst

Bijlage 1 Lijst met minimaal benodigde middelen/diensten van leverancier

Applicatiedienstverlening

De dienstverlener levert toegang tot de software via internet, inclusief:

- functionaliteit van de applicatie, te gebruiken op devices zoals telefoons en tablets, als ook op een desktop pc.
- updates, nieuwe releases en bugfixes
- configuratiemogelijkheden
- gebruikers- en rollenbeheer

Hosting en Technische Infrastructuur

De dienstverlener verzorgt volledig de onderliggende techniek:

- hosting van de applicatie en databases (OTAP)
- schaalbaarheid en performance
- beschikbaarheid van de dienst
- monitoring van de systemen

Beveiliging

De dienstverlener zorgt voor de beveiliging van:

- data (encryptie, toegang, logging)
- accounts (MFA, SSO, identityintegraties)
- de infrastructuur (patching, kwetsbaarheidsbeheer)
- naleving van relevante standaarden zoals AVG

Data-beheer

De dienstverlener verzorgt:

- veilige opslag en beheer van gegevens
- back-ups en herstel mogelijkheden (disaster recovery)
- datatoegankelijkheid en exportmogelijkheden
- afspraken over bewaartermijnen en verwijdering

Integraties en API's

De dienstverlener verzorgt:

- API's of standaardkoppelingen met andere systemen
- documentatie en ondersteuning bij integratie

Ondersteuning & Servicemanagement

De dienstverlener verzorgt:

- de servicedesk / ondersteuning voor incidenten en vragen
- een kennisbank en documentatie
- duidelijke afspraken over responstijden (*Service Level Agreement*)
- beheer van updates en gepland onderhoud

Contractuele en compliancediensten

De dienstverlener verzorgt duidelijkheid over:

- SLA's (uptime, performance, responstijden)
- verwerkersovereenkomst (AVG)
- audit- en compliance-informatie
- transparante tarieven en licentiebeheer

Bijlage 2 Lijst van functionaliteiten en onderdelen voor het Programma van Eisen op hoofdlijnen

Onderstaande functionaliteiten en onderdelen (in de tabellen) zijn een aanvulling en/of specificatie op de tekstuele beschrijving van het Programma van Eisen op hoofdlijnen in hoofdstuk 5. Deze kunnen worden gebruikt in voorbereiding op een eventuele aanbesteding (fase 3).

Functie	Uitwerking
1. Algemeen	- Beschrijving van het systeem/ doel - Beschrijving van de uitgangspunten - Vereiste/ gewenste koppelingen met ander(e) syste(e)men

Deel A: Registreren (fysiek, digitaal), traceren, matchen en volgen

Functie	Uitwerking
2. Registratie van getroffen en, verwanten en vermisten	Gedetailleerde informatie over de getroffen en, verwanten en vermisten. Zie voor indicatie van (typen) gegevens de tabel in het hoofdstuk van de juridische quickscan. Exacte benodigde gegevens zullen in samenspraak met de stakeholders worden afgesproken.
	- Vereiste randvoorwaarden: - Uploaden van lijsten (passagierslijsten, opvanglocatie) - Registratie/aanmaken van een persoonsdossier ook mogelijk als niet alle velden ingevuld zijn (bijvoorbeeld het ontbreken van een geboortedatum)
	Het maken van een unieke code (bv QR- of Barcode) voor getroffen en
	Registratie van verwanten en de gezochte naasten (vermisten), zodat er een koppeling in het systeem gelegd kan worden tussen de dossiers van verwanten en vermisten/getroffen en.
	Registratie van getroffen en via online zelfregistratiemodule (burgers kunnen zelf hun eigen gegevens invoeren)
3. Registratiepunten	Registratie van getroffen en via algemene registratiepunten (call-center/frontoffice SIS,

Functie	Uitwerking
	opvanglocatie, ziekenhuis, zelfregistratie, plaats incident) en incident specifieke registratiepunten (zoals lokale steunpunten bij een gemeente of een brandweerkazerne)
	• Randvoorwaarden: - o Mogelijkheid om registratiepunt via API op te laden (bijvoorbeeld namen van ziekenhuizen) in een casus - o Mogelijkheid om naamgeving aan te passen - o Mogelijkheid om nieuwe registratiepunten toe te voegen/aan te maken in een casus
	• Online registratiemodule voor het registreren van vermisten/zoekvragen door verwanten, die terecht komen bij de backoffice van SIS (digitale registratie van "SIS/ikzoekmijnnaaste"). Matches kunnen gedaan worden op basis van deze registratie met de vermisten.
5. Online zoekvragen	• De veiligheidsregio/ gemeente kunnen een online web gebaseerde registratiemodule activeren ten behoeve van zoekvragen voor vermisten. De zoekvraag gaat via persoonlijke gegevens (check roadmap)
6. Online zelfregistratie	• De veiligheidsregio/ gemeente kunnen een online web gebaseerde registratiemodule activeren ten behoeve van zelfregistratie van getroffenen. • Bij registratie krijgt getroffene een unieke code • Registratie 'ik ben veilig'
	• Randvoorwaarde: de zelfregistratiemodules (systeem) kunnen afzonderlijk worden opgestart en staan los van het getroffenenregistratiesysteem (veiligheidseis)
7. Telefonische registratie (frontoffice SIS)	• Telefonische registratie van vermisten. Zowel getroffenen als verwanten kunnen een zoekactie starten.
8. Incidenten	• Na creatie (zie punt 10) kunnen een of meerdere lijsten van potentiële slachtoffers ingeladen worden, vanuit bv passagierslijsten oid.
9. Traceren	• De real-time actuele locatie van een getroffene wordt weergegeven en actualiseert automatisch bij een nieuwe registratie/aankomst op een andere locatie

Functie	Uitwerking
10. Matchen (backoffice SIS)	Het systeem moet de beschikbare informatie over niet zelfredzame slachtoffers kunnen matchen met als resultaat een slachtoffer-, vermisten- en dodenlijst

Deel B: Systeembeheer en administratieve functies

Functie	Uitwerking
11. Incidenten	Beheerder moet incident/casus kunnen aanmaken, bewaren en verwijderen (functionele eis)
12. Identiteits- en toegangsbeheer	Het systeem heeft een toegangsbeheersfunctie: • Aanmaken, wijzigen en verwijderen van accounts • Rechten- en roltoewijzing (RBAC) • Attribuuutbeheer (naam, e-mail etc) • Activiteiten logging
13. Management-functies	Door middel van groepscode kunnen groepen zoals verwanten en vermisten gegroepeerd worden.
14. Auditing	Het systeem voorziet in een centrale auditing die van toepassing is op zowel het getroffenregistratiesysteem als de (zelf)registratiemodules.
15. Rollen en rechten	Het systeem biedt gebruikers, die een specifiek profiel (functie), toegang door middel van rollen. Het systeem laat toe dat een profiel/ functie meerdere rollen kan hebben.
16. Technische Eisen	Het systeem beschrijft op welke wijze de volgende onderdelen zijn geregeld: • Architectuur en hosting De basis waarop en hoe de dienst technisch is opgebouwd: • Beveiliging (security) Alle maatregelen rondom beveiliging, van encryptie tot kwetsbaarheidsbeheer • Identiteit en toegangsbeheer (IAM) Authenticatie, autorisatie en koppeling met externe identity providers (waaronder TGV) • Data en Datamanagement Datakwaliteit, datalocatie, lifecycle, integriteit en opslag • Back-up, herstel en continuïteit Back-ups, disaster recovery, RTO/RPO en continuïteitsafspraken • Integraties en API's Technische koppelvlakken, data-uitwisseling en standaardprotocollen • Applicatiebeheer en updates Updates, releases, onderhoudsvensters en versiebeheer

Functie	Uitwerking
	• Performance en capaciteit Snelheid, schaalbaarheid en beschikbaarheid • Logging, monitoring en audit Audittrails, foutlogging, monitoring, export mogelijkheden (SIEM) • Privacy en compliance AVG, verwerkersovereenkomst, auditmogelijkheden • Support en servicemanagement Incidentafhandeling, SLA-afspraken, servicelevels en documentatie • Exit strategie • Data-export, migratie, exit proces
17. Opleiden en oefenen	Het systeem heeft een oefenomgeving dat gebruikt kan worden voor opleidingen en trainingen

Deel C: Informeren en communiceren

Functie	Uitwerking
18. Statusrapporten	Het systeem biedt de mogelijkheid om per incident diverse rapporten (numerieke overzichten) te genereren. Dit is afhankelijk van de functie van de gebruiker: • Algemeen situatierapportage - o Triage - o Pre-triage - o Overzicht aantal getroffen en verwanten (zowel via registratiepunt, als online en welke de hulpverlening hebben verlaten/ op weg naar huis) - o Groepscode? • Rapportages met aantallen personen geregistreerd per geactiveerd registratiepunt • Rapportages met focus op (gesorteerd op) nationaliteiten • Rapportages met aantallen gezochte personen/ (openstaande) zoekvragen • Rapportages met aantallen overleden personen • Rapportages met aantallen gewonde personen
20. Dashboard	Het systeem bevat een weergave van een dashboards: • Commando post dashboard Globaal overzicht (aantallen slachtoffers (incl. triage classificatie)/verwanten/getuigen, telefoontjes (zoekvragen), aantallen per locatie of onderweg, etc)

Functie	Uitwerking
	voor de functionele eigenaren (GZ en BZ), informatie ten behoeve van het CoPI en ROT. Exacte weergave van gegevens in dit dashboard moet verder uitgewerkt worden met de stakeholders.
21. Lijsten	• Het systeem kan verschillende lijsten (inclusief de juiste toegang) genereren: - o Lijsten met geregistreerde getroffen en per (geactiveerd) registratiepunt - o Totaallijst van alle getroffen en - o Lijst van vermisten, gekoppeld aan verwanten (geregistreerde gegevens). - o Lijst met zelfgeregistreerde getroffen en - o Slachtofferlijst - o Vermistenlijst - o Lijst met overledenen



Rijksinstituut voor Volksgezondheid
en Milieu
*Ministerie van Volksgezondheid,
Welzijn en Sport*



Dit is een uitgave van:

**Rijksinstituut voor Volksgezondheid
en Milieu**

Postbus 1 | 3720 BA Bilthoven
www.rivm.nl

Nederlands Instituut Publieke Veiligheid

Postbus 7010 | 6801 HA Arnhem
www.nipv.nl

september 2026