

Algemene AVG kaders verkeerskundig onderhoud en analyse

LVMB

Definitief

27 maart 2024



Algemene AVG kaders bij het verrichten van verkeerskundig onderhoud en analyse

Dit document beschrijft de algemene kaders voor onderzoek en analyse door de wegbeheerder ten behoeve van verkeerskundig onderhoud gelet op eisen uit de Algemene verordening gegevensbescherming (AVG). Wegbeheerders maken voor hun publieke taken als wegbeheerder onder meer gebruik van iVRI's en VRI's. Met dergelijke systemen en inrichtingen worden gegevens verwerkt, waaronder in een beperkt aantal gevallen ook gegevens die als persoonsgegevens gekwalificeerd kunnen worden. Denk hierbij aan de tijdelijke pseudo-ID bij iVRI's, herleidbare gegevens in opgeslagen camerabeelden bij cameradetectie, of indirect herleidbare gegevens als lijnnummers, snelheid, positie en locatie. In het geval er sprake is van een persoonsgegeven moet worden gehandeld conform de AVG.

Bij verkeerskundig onderhoud zal er bijvoorbeeld sprake zijn van het bewaken, analyseren en het beheren van de juiste verkeerskundige werking van verkeerssystemen. Hiervoor is het noodzakelijk dat er analyses worden gemaakt. Deze analyses vinden plaats op basis van data die is verkregen bij onder meer de toepassing van zowel iVRI's als VRI's, maar ook middels andere sensoren. Dit betekent, dat op basis van de AVG de data reeds is verzameld (verwerkt) voor een 'oorspronkelijk' doel. Voor het verkeerskundig onderhoud wordt die data gebruikt voor onder meer:

- De controle van de datakwaliteit
- Diagnostiek
- Statistisch onderzoek naar kruispunten en trajecten
- KPI's voor kruispunten en trajecten

Als dit persoonsgegevens betreffen, is het op grond van de AVG onder voorwaarden rechtmatig die gegevens voor die onderzoeksdoeleinden verder te gebruiken. Hieronder worden de stappen beschreven, waar de wegbeheerder bij het uitvoeren van analyses voor verkeerskundig onderhoud rekening mee moet houden:

Stap 1: bepaal eerst of er sprake is van persoonsgegevens

Voor het uitvoeren van het specifieke analyse voor verkeerskundig onderhoud moet eerst worden bepaald of de data die wordt gebruikt voor de analyse direct of indirect herleidbare persoonsgegevens betreft.

Onder de AVG wordt een persoonsgegeven gedefinieerd als informatie over een geïdentificeerde of identificeerbaar natuurlijk persoon. Het gaat om informatie over een persoon van wie de identiteit duidelijk is of aan de hand van aanvullende informatie kan worden vastgesteld. Dus, elk soort informatie kan een persoonsgegeven zijn, mits het betrekking heeft op een geïdentificeerde of identificeerbaar persoon. Het uitgangspunt is dat bij statistische analyses, zoals ten behoeve verkeerskundig onderzoek, wordt gewerkt met het zowel ontvangen als analyseren van **geanonimiseerde gegevens**. Dit omdat in dat geval de AVG ook niet van toepassing is.

Let op: het gaat dus om de data die gebruikt gaat worden voor de analyse ten behoeve van het verkeerskundig onderhoud! Deze kaders zien niet op het verstrekken van datasets aan derden, zoals politie en verzekeraars!

Beoordeel of er sprake is van een dataset die – bijvoorbeeld in een database – persoonsgegevens bevat. Als die dataset (of een deel daarvan) gebruikt gaat worden voor verdere analyse ben je persoonsgegevens aan het verwerken! Daarvan is ook sprake indien je die specifieke persoonsgegevens voorafgaand aan de analyse *eerst* gaat anonimiseren of pseudonimiseren. Ook de handeling van anonimiseren of pseudonimiseren is een verwerking van persoonsgegevens. Die handeling moet volgens de kaders van de AVG ook rechtmatig zijn.

Om vast te stellen of een persoon identificeerbaar is, moet rekening worden gehouden met alle redelijke middelen die kunnen worden gebruikt om de persoon direct of indirect te identificeren. Identificatie vereist dus elementen die een persoon zodanig beschrijven dat hij of zij kan worden onderscheiden van alle andere personen en als individu kan worden herkend. De naam van een persoon of een kenteken zijn voorbeelden hiervan en kunnen een persoon eenvoudig direct identificeren.

Bij indirect geïdentificeerde of identificeerbare personen gaat het doorgaans om een aantal 'unieke combinaties'. In gevallen waarin het op het eerste gezicht niet mogelijk is met de beschikbare identificatiemiddelen één bepaalde persoon te onderscheiden, kan die persoon wellicht toch identificeerbaar zijn doordat aan de hand van die informatie in combinatie met andere gegevens (die al dan niet bij de wegbeheerder rusten) de betrokkene van andere personen kan worden onderscheiden. **Let op:** hiervan is ook sprake indien het gegeven niet door de

wegbeheerder zelf kan worden herleid tot een bepaald persoon, maar dit vanwege het combineren van gegevens uit andere bronnen mogelijk is. Eind 2023 heeft de afdeling bestuursrechtspraak van de Raad van State ten aanzien van V-log data geoordeeld dat dit persoonsgegevens betreffen: *De V-log data geven inzicht in het gedrag en de locatie van een individuele weggebruiker. Weliswaar zijn de data op zichzelf genomen niet direct te relateren tot individuele personen, maar die data kunnen op basis van aanvullende gegevens wel worden gekoppeld aan geïdentificeerde of identificeerbare natuurlijke personen.*¹ Kortom, net als V-log data zullen ook CAM-, SRM- en SSM-berichten persoonsgegevens bevatten.

Let op: of het een persoonsgegevens betreft, moet worden beoordeeld of het 'gegeven' herleidbaar kan zijn tot een persoon. Daarbij moet je niet redeneren vanuit enkel of het voor de eigen organisatie, de wegbeheerder dus, direct of indirect herleidbaar is. Dit moet breder worden getrokken, waarbij moet worden beoordeeld of de data – al dan niet in combinatie met andere data – voor andere organisaties (waar een relatie mee kan zijn) eventueel herleidbaar wordt.

Gepseudonimiseerde persoonsgegevens die door het gebruik van aanvullende gegevens aan een natuurlijke persoon kunnen worden gekoppeld, moeten als gegevens over identificeerbare natuurlijke persoon worden beschouwd. Persoonsgegevens bevatten attributen, zoals naam, locatie, GPS, kenteken, of andere elementen die tot identificatie kunnen leiden. Het proces van het pseudonimiseren van persoonsgegevens houdt in dat deze attributen worden vervangen door een pseudoniem. Persoonsgegevens kunnen dan niet langer aan een specifieke betrokkene worden toegeschreven zonder dat gebruik wordt gemaakt van aanvullende informatie, mits deze aanvullende informatie afzonderlijk wordt bewaard en er waarborgen zijn geïmplementeerd dat de persoonsgegevens niet aan een natuurlijke persoon worden toegeschreven. In tegenstelling tot anonieme gegevens, zijn gepseudonimiseerde gegevens nog steeds persoonsgegevens en vallen zij dus onder de AVG.

Zo is het pseudo-ID bij de iVRI's volgens de Ketenbrede PIA publiek-private dataketen iVRI's voor wegbeheerders of ITS-leveranciers niet herleidbaar tot een persoon of voertuig. Echter, het is wel een persoonsgegeven! Het pseudo-ID kan bijvoorbeeld gelet op het bezit van camerabeelden bij de wegbeheerder, de organisatie waar de wegbeheerder onder valt of een derde, zoals politie, wel herleidbaar zijn tot een individu.

Ook zou de overige data als locatie, tijd en snelheid in combinatie met andere gegevens die bij de wegbeheerder of een andere organisatie aanwezig is, kunnen worden gecombineerd. Denk hierbij aan camerabeelden of vanwege de weinige verkeersbewegingen en de specifieke – bijvoorbeeld hoge – snelheid van een 'voertuig' bij meerdere (i)VRI's. Maar denk ook aan het lijnnummer of personele informatie van de berijders waar een organisatie ook over beschikt. Als die data met locatie, datum en tijd niet wordt geaggregeerd in een rapportage en deze rapportage wordt gepubliceerd of gedeeld met die specifieke organisatie, is identificatie dus (alsnog) mogelijk!

Ter illustratie:

Bij het verrichten van verkeerskundige analyses op basis van CAM-data uit de UDAP zal er gelet op de onderstaande dataset op basis van het stationID geén sprake zijn van herleidbare persoonsgegevens indien:

- deze specifieke set aan gegevens uitsluitend voor het doel worden gebruikt van de verkeerskundige analyse; én
- niet verder worden verrijkt/gecombineerd met andere (persoons)gegevens waardoor de data wel tot een individu herleidbaar kan zijn; én
- de resultaten van de verkeerskundige analyse op voldoende hoog niveau worden geaggregeerd; én
- de dataset die voor de analyse is gebruikt wordt vernietigd zodra deze niet meer nodig is, dan wel niet toegankelijk wordt gemaakt voor andere doeleinden of niet verstrekt derden.

Denk bij aanvullende informatie aan camerabeelden of proces-verbalen. Het advies is om de onderstaande stappen, met name Stap 2 t/m 6 en 8 gelet op maatregelen, door te lopen. Waar vereist dienen dan de maatregelen te worden getroffen zoals daar staan opgesomd.

stationID	logtimestamp	vri	stationType	latitude	longitude	heading_deg	speed_kmh	gpsAccuracyMajor_m	gpsAccuracyMinor_m	generationDeltaTimestamp
132914512	10:41:21,293	7aa6003c	4	52,22274	4,862587	118	64,98	40,95	40,95	09:41:16,474
132914512	10:41:22,298	7aa6003c	4	52,22265	4,862838	118	64,98	40,95	40,95	09:41:17,469
132914512	10:41:23,290	7aa6003c	4	52,22258	4,863074	119	64,98	40,95	40,95	09:41:18,457
132914512	10:41:24,222	7aa6003c	4	52,22248	4,863342	119	65,988	40,95	40,95	09:41:19,463

¹ Afdeling bestuursrechtspraak Raad van State, 20 december 2023, ECLI:NL:RVS:2023:4752, r.o. 4.

Als er sprake is van persoonsgegevens of indien niet kan worden uitgesloten of de te gebruiken dataset persoonsgegevens bevat al dan niet in combinatie met gegevens beschikbaar binnen de eigen of een andere organisatie, dan moeten de onderstaande stappen worden gevolgd:

Stap 2: bepaal het doel en de grondslag van de analyse

Een analyse of onderzoek ten behoeve van verkeerskundig onderhoud dient een bepaald **doel**. Op basis van het doel moet worden bepaald of de persoonsgegevens die je wilt gaan analyseren wel nodig zijn om het onderzoeksdoel te bereiken. Daarbij is het noodzakelijk dat je dit altijd beoordeeld vanuit het doel waarvoor de data die je gebruikt voor de analyse oorspronkelijk zijn gebruikt/verkregen. De reden hiervoor is dat het doel van de analyse 'verenigbaar' moet zijn met het doel waarvoor je de onderzoeksdata in eerste instantie hebt verkregen. Is het logisch en ligt het voor de hand dat die verkeersgegevens worden gebruikt voor een analysedoel, dan mag je die data ook voor het onderzoek gebruiken.

Beschrijf daarom altijd waarom je het onderzoek uit moet voeren: - wat is het doel van het onderzoek, - op basis van welk doel de onderzoeksdata (bijvoorbeeld de verkeersgegevens) zijn verkregen, - en of dat strookt met het doel waarvoor de onderzoeksdata in eerste instantie zijn ontvangen/verkregen?

Denk hierbij aan de volgende analyse-/onderzoeksdelen:

- het analyseren of er op correcte wijze prioriteit wordt gegeven aan bepaalde doelgroepen (zoals ambulances);
- het analyseren of op basis van CAM data de ITS applicatie (eerder of langer groen licht) reageert op de gespecificeerde manier;
- het analyseren wat het effect is op de doorstroming (bv. wachttijden) van de te prioriteren doelgroep en andere verkeersdeelnemers op het kruispunt;
- het op basis van de analyse verbeteren van de instellingen van de ITS applicatie en/of verbeteren van de datakwaliteit om tot betere prestaties te komen.

Bepaal vervolgens ook op basis waarvan je het onderzoek uitvoert. Dit is de zogenaamde **grondslag** van de verwerking. Het doel van het onderzoek moet hierop gebaseerd zijn.

In de regel zal de grondslag van de analyse voor het verkeerskundig onderhoud gebaseerd zijn op:

a. Onderzoek vanwege een taak van algemeen belang of openbare orde

Het gaat hierbij om taken van de wegbeheerder die ergens in de wet zijn vastgelegd. Voor wegbeheerders volgt deze taak specifiek uit de Wegenverkeerswet, namelijk de artikelen 2 (o.a. zorgdragen voor de verkeersveiligheid en bruikbaarheid van de weg), en 18 (verkeersbesluiten). In die wet staat niet expliciet dat persoonsgegevens moeten worden verwerkt. Zo zal je als wegbeheerder zorg moeten dragen voor de juiste werking van de gebruikte iVRI en VRI inrichtingen en applicaties. Dit moet je monitoren, evalueren, controleren en waar vereist ook verbeteren gelet op die publieke (algemene) taak. Ook kan deze grond worden gebruikt voor het in kaart brengen en rapporteren van hoog geaggregeerde gegevens (niet herleidbaar tot individuen) om het verkeerveiligheidsbeleid te kunnen aanpassen of bijstellen.

Andere – minder voorkomende – mogelijkheden voor de wegbeheerder zouden nog kunnen zijn:

b. Onderzoek vanwege een wettelijke verplichting:

Als een onderzoek moet worden uitgevoerd, omdat dit in een wet is voorgeschreven, voer je het onderzoek uit omdat een wet (of lagere regeling) dit verplicht.

c. Onderzoek met voorafgaande toestemming

Als er geen sprake is van één van de bovengenoemde grondslagen, dan zou je alsnog op basis van voorafgaande toestemming van de respondent een onderzoek kunnen verrichten. Het is wel van belang dat de respondent vooraf duidelijk wordt geïnformeerd over waarvoor men toestemming geeft (doel onderzoek), welke gegevens (bij voorkeur geanonimiseerd) worden verwerkt, wanneer de persoonsgegevens worden vernietigd, en dat men de mogelijkheid heeft om de toestemming in te trekken. Denk hierbij aan enquêtes of interviews.

Stap 3: bepaal wie verantwoordelijk is voor het verkeerskundig onderhoud of de analyse

Het is belangrijk om te bepalen welke positie je als wegbeheerder inneemt bij het uitvoeren van de analyses ten behoeve van het verkeerskundig onderhoud. Het verrichten van verkeerskundig onderhoud is de

verantwoordelijkheid van de wegbeheerder. Indien het onderhoud en/of de analyse intern wordt uitgevoerd, dan is en blijft de wegbeheerder **verwerkingsverantwoordelijk** voor het zorgvuldig omgaan met persoonsgegevens.

Extern bureau:

Maak je gebruik van een extern bureau voor het (deels) uitvoeren van het onderhoud en de analyse, dan verwerken zij in opdracht van de wegbeheerder (of het LVMB) deze gegevens. Anderzijds kan het ook zijn dat je als wegbeheerder voor andere organisaties het onderhoud en/of de analyse coördineert of uitvoert. Beide situaties hebben een belangrijke consequentie. Als de wegbeheerder een opdracht verstrekt dan is de wegbeheerder **verwerkingsverantwoordelijke** en is de opdrachtnemer (het onderzoeksbureau) de **verwerker**. In het geval de wegbeheerder (of het LVMB) een onderzoek uitvoeren voor andere organisaties zijn de rollen omgedraaid. In dat geval is de wegbeheerder **verwerker** en de “opdrachtgever” is dan **verwerkingsverantwoordelijke**.

Als er sprake is van een analyse waarbij alleen geanonimiseerde gegevens worden aangeleverd en verwerkt, is geen verwerkersovereenkomst nodig. In het geval van gepseudonimiseerde persoonsgegevens moet wel een verwerkersovereenkomst worden gesloten.

Stap 4: bepaal welke gegevens noodzakelijk zijn voor het onderzoeksdoel

Zoals gezegd, het uitgangspunt is dat ten behoeve van (verkeerskundige) statistische analyses wordt gewerkt met het zowel ontvangen als analyseren van **geanonimiseerde gegevens**. Dit omdat in dat geval de AVG ook niet van toepassing is. Mocht het vanwege het doel van het onderzoek niet mogelijk zijn om te anonimiseren, dan dien je uit te gaan van alleen die data die noodzakelijk is om het doel van het onderzoek te bereiken. Ga in dat geval eerst uit van **pseudonimiseren van de gegevens op een passend niveau**.

Mocht dat ook niet mogelijk zijn, dan zal je moeten verantwoorden waarom je bepaalde **ruwe data** die niet geanonimiseerd of gepseudonimiseerd is als onderzoeksgegevens moet gebruiken.

Bij het **anonimiseren** van persoonsgegevens dient te worden voldaan aan de volgende drie voorwaarden:

1. Gegevens moeten niet herleidbaar zijn tot een natuurlijke persoon (een natuurlijke persoon direct of indirect identificeren); en,
2. Gegevens moeten niet-koppelbaar zijn, dit betekent dat gegevens niet in verband kunnen worden gebracht met opgeslagen gegevens van een natuurlijke persoon; en,
3. Gegevens moeten niet-deduceerbaar zijn, dit betekent dat uit de gegevens geen gegevens kunnen worden afgeleid van een natuurlijke persoon tenzij dit een onevenredige hoeveelheid geld, tijd, mens- en/of computerkracht kost.

Het is verstandig om onderzoeksgegevens die nodig zijn vanuit interne afdelingen, dan wel derden, versleuteld aan te laten leveren (of vice versa). Daarbij geniet het sterk de voorkeur om in het geval onderzoeksgegevens die tot een persoon herleidbaar (kunnen) zijn, deze te laten anonimiseren of middels een sleutel te pseudonimiseren op hoog geaggregeerd niveau. In dat laatste geval is het verstandig de sleutel na aanlevering door de desbetreffende afdeling of partij te laten vernietigen. Op die wijze zijn de onderzoeksgegevens niet meer herleidbaar.

Gelet op analyses ten behoeve van verkeerskundig onderhoud zal er in de praktijk géén sprake zijn van bijzondere persoonsgegevens (zoals medische gegevens). Mocht daar wel sprake van zijn, neem dan contact op met de privacy deskundige binnen de organisatie.

Stap 5: bepaal welke maatregelen worden getroffen ter bescherming van gegevens

Als er persoonsgegevens voor het onderzoek worden ontvangen, zal je passende beveiligingsmaatregelen moeten nemen om deze gegevens te beschermen. Hoe gevoeliger de gegevens hoe zwaarder de maatregelen moeten zijn. Wees altijd kritisch en bepaal 1: welke gegevens je nodig hebt en ook aangeleverd krijgt (niet meer dan nodig) én 2. neem passende maatregelen om die gegevens goed te beveiligen. Denk hierbij aan maatregelen hoe de voor de analyse benodigde dataset ‘veilig’ beschikbaar wordt gesteld of verzonden/verstrekt aan de onderzoeker(s), dat alleen personen die het onderzoek uitvoeren toegang hebben tot de gegevens, dit ook op afgeschermd schijven of applicaties met beperkte autorisaties wordt ingericht en opgeslagen, en de onderzoeksgegevens te vernietigen zodra deze niet meer nodig zijn, zoals in ieder geval wanneer de analyse heeft plaatsgevonden.

Bepaal en beschrijf met betrekking tot maatregelen dus de volgende onderdelen:

1. De systemen waarmee het onderzoek wordt uitgevoerd.
2. De wijze waarop de onderzoeksgegevens (ruwe data) worden verkregen;
3. De wijze waarop de onderzoeksgegevens (ruwe data) worden verzonden/verstrekkt aan de 'onderzoekers';
4. Wordt er gebruik gemaakt van versleutelingstechnieken, en zo ja welke en op welke wijze wordt dit toegepast?
5. Waar wordt de verkregen onderzoeksgegevens (ruwe data) opgeslagen?
6. Wie heeft toegang tot de onderzoeksgegevens (ruwe data)?
7. Wanneer worden de onderzoeksgegevens (ruwe data) vernietigd?
8. En op welke wijze is geborgd dat de vernietiging ook daadwerkelijk plaatsvindt?

Stap 6: het beoordelen van de voorgenomen analyse door de privacy deskundige

Nadat je de stappen 1 tot en met 5 hebt doorlopen en beschreven in een document. Leg dit dan ter controle voor aan de de privacydeskundige binnen de organisatie. Diegene kan dan toetsen of het onderzoek/de analyse voor het verkeerskundig onderhoud voldoet aan de AVG.

Voor structurele of veel voorkomende analyses kun je daar afspraken over maken, zodat slechts bij wijzigingen dit opnieuw intern kan worden getoetst en vastgelegd. Bij incidentele analyses is het advies dit telkens vooraf te laten toetsen én ook vast te leggen. Met de vastlegging kan worden verantwoord hoe de wegbeheerder bij de analyse(s) voldoet aan de AVG.

Stap 7 (indien van toepassing): Het uitzetten van een onderzoek bij respondenten

Als je geen gebruik maakt van bestaande gegevens, maar moet je deze informatie nog verkrijgen van respondenten, dan moet je rekening houden met de volgende zaken:

- Bij zowel steekproeven als op andere wijze waarop gegevens van respondenten worden gebruikt om hen voor deelname uit te nodigen, is het van groot belang dat je de adresgegevens van de respondenten strikt scheidt van de ontvangen onderzoeksgegevens. Dit om ervoor te zorgen dat de onderzoeksgegevens niet herleidbaar zijn tot individuen die op basis van de geselecteerde respondenten en adressen zijn aangeschreven of uitgenodigd.
- Voor onderzoeken die betrekking hebben op algemeen belang en het onderzoeken van de doelmatigheid van een beleid dat tot de taken van de wegbeheerder behoort, denk bijvoorbeeld aan beleid m.b.t. verkeersveiligheid of aanleg nieuw tracé, kun je als wegbeheerder (m.n. gemeenten) een a-selecte steekproef laten trekken uit de Basisregistratie Personen (BRP). Een andere mogelijkheid is een mailing te versturen op adresniveau, waarbij je de respondenten – niet op naam – uitnodigt om deel te nemen aan een onderzoek, bijvoorbeeld een enquête;
- Voor statistisch onderzoek geldt dat het onderzoek beoogt uitspraken te doen op niet-individueel identificeerbaar niveau. Waarbij identificeerbare gegevens alleen met expliciete toestemming van de respondent worden opgenomen in de rapportage. Werk dus bij voorkeur met geanonimiseerde data en neem alleen identificeerbare gegevens op indien de respondent vooraf toestemming heeft gegeven;
- Zorg ervoor dat adreslijsten van de benaderde respondenten altijd separaat worden gehouden van de onderzoeksgegevens. Bij voorkeur opslaan op een andere schijf met strikte scheiding, zodat ook de degene die de onderzoeken uitvoeren/analyseren geen toegang hebben tot de adreslijsten.

Stap 8: het presenteren/rapporteren van een onderzoek

Voordat je het onderzoek gaat rapporteren en/of presenteren, dien je goed na te denken over de wijze waarop je de resultaten gaat rapporteren en/of presenteren. Houd hierbij rekening met de volgende **uitgangspunten**:

1. Aggregeer op voldoende hoog niveau, zodat individuen niet identificeerbaar zijn. Of iets voldoende hoog is, hangt van de context af waarbinnen je gegevens verwerkt. Denk hierbij aan rapportages op Station ID of locatieniveau waarbij de aantallen dusdanig gering zijn dat gelet op de context is te achterhalen, bijvoorbeeld op basis van lijnummers in combinatie met locaties of bij enquêtes de respondenten, wie de desbetreffende persoon is of kan zijn. In die gevallen zal je dus op een hoger niveau moeten aggregeren;

2. Rapportage vindt in principe altijd plaats op basis van de verkeerssituatie, de inrichtingen, de applicaties, doelgroepen of populaties;
3. Rapportage op individueel niveau vindt enkel en alleen plaats na voorafgaande ondubbelzinnige, voldoende geïnformeerde, schriftelijk of elektronisch vastgelegde toestemming. Daarbij dien je de volgende zaken altijd mee te nemen voorafgaand aan, in en na afloop van de rapportage:
 - a. Verstrek – voorafgaand aan de start van het onderzoek – voldoende informatie over soorten van persoonsgegevens, de categorieën van ontvangers, zoals de opdrachtgever, aan wie identificerende gegevens worden verstrekt en voor welke doeleinden.
 - b. Communiceer de informatie schriftelijk (of elektronisch), en zorg dat informatie eenvoudig kan worden geraadpleegd.
 - c. In het geval van onderzoek met data van respondenten: zorg voor een mogelijkheid om de data van de respondenten te vernietigen. Als respondenten namelijk besluiten dat hun gegevens niet gebruikt mogen worden (intrekking van toestemming), dan mag de data niet worden gebruikt voor de rapportage en dient deze te worden vernietigd.

Stap 9: Het delen van de onderzoeksgegevens

In bepaalde gevallen kan het voorkomen dat derden vragen om de onderzoeksgegevens. Deel geen onderzoeksgegevens die herleidbaar zijn tot individuen, tenzij je wettelijk verplicht bent om die gegevens te delen. Bijvoorbeeld naar aanleiding van een formeel verzoek (vordering) vanuit het Openbaar Ministerie/politie. Als je besluit om wel onderzoeksgegevens te delen, deel dan alleen geanonimiseerde data.

Voor wat betreft rapportages kun je deze delen zolang deze geanonimiseerd dan wel op zeer hoog niveau geaggregeerd zijn.