



aan Management DRI, CPO

van 5.1.2.e

onderwerp Overzicht privacy issues binnen DRI – nulmeting 2022

datum 15 november 2021

Dit document geeft inzicht in privacy aspecten binnen DRI. Dit is geen allesomvattende evaluatie, maar tracht een eerste beeld te schetsen van zaken waar de privacy coördinator op dit moment zicht op heeft. Deze zaken zijn opgehaald binnen de organisatie in de periode oktober/november 2021.

Deze inventarisatie wordt gedeeld met de CPO. Specifieke privacy casussen kunnen worden overgenomen in een centrale kennis database, die door CPO en privacy coördinatoren wordt opgebouwd. Niet alleen om nieuwe casussen tegenaan te houden om te voorkomen dat het wiel opnieuw wordt uitgevonden, maar ook om naar buiten toe beter te kunnen aangeven wat het CBS vanuit haar beleid ten aanzien van privacy allemaal doet en dat dit afdoende doordacht gebeurt.

DVZ

Gegevens die vanuit data verzamelen worden ontvangen worden direct doorgezet naar statistiekafdelingen. Grotendeels via een geautomatiseerd en vanuit ICT beveiligde proces. Binnen secundaire waarneming zijn de ervaringen met verschillende trajecten voor het binnenhalen van nieuwe databronnen vanuit andere organisaties, dat de CBS expertise en procesinrichting op het gebied van beveiligd up- en downloaden van data bestanden veelal beter is dan in andere organisaties.

Gegevens vanuit primaire waarneming worden via de waarneemkanalen CAWI, CATI en CAPI verzameld. Bij de laatste 2 wordt de medewerker die uitvraagt via de voorliggende vragenlijst geconfronteerd met privacy gevoelige informatie. Na de invoer van de informatie in de CATI en CAPI systemen wordt die informatie beveiligd weggeschreven en verwerkt binnen DVZ met zeer beperkte toegang van medewerkers. Gegevens worden vrijwel meteen intern doorgezet naar statistiekafdelingen.

Jaarlijks ondergaan de kanalen een pentest door een externe organisatie.

Het proces van data verzamelen is opgedeeld in deelprocessen waarbij teammanagers toezien op periodieke uitvoering van T baseline toetsen - waar in het proces worden persoonsgegevens verwerkt en wat zijn de risico's dat privacy gevoelige informatie in verkeerde handen komt. Waar dat speelt wordt het aantal medewerkers dat toegang heeft tot dergelijke gegevens beperkt via autorisatieprocedures (periodiek geven teammanagers aan wie toegang heeft tot bepaalde processtappen) en er wordt toegezien op naleving van afgesproken bewaartermijnen voor specifieke bestanden in het proces van dataverzamelen (zie bijlage 1.)

Daarnaast hebben medewerkers standaard een geheimhoudingsplicht (onderdeel arbeidsovereenkomst) en worden gegevens zo snel mogelijk binnen de statistische processen geanonimiseerd.

Voor een overzicht van specifieke privacy gevoeligheden en noodzakelijke beheersmaatregelen binnen DVZ wordt verwezen naar bijlage 2.



Het proces binnen DVZ wordt ondersteund vanuit het Phoenixsysteem dat recentelijk is opgeleverd en waarbij ook invulling wordt gegeven aan automatische vernietiging van gegevens. Als basis daarvoor is onder andere een nota opgeleverd waarin de AVG is uitgewerkt en wat daarvan de consequenties zijn voor de werkwijze binnen DVZ, inclusief maatregelen die nodig zijn om privacy afdoende te borgen. Die maatregelen zijn geïmplementeerd.

DRD

DRD draagt vanuit methodologie en procesontwikkeling bij aan innovatie binnen het CBS, vooral gericht op het verbeteren en innoveren van bestaande statistische processen en het maken van nieuwe statistieken. DRD heeft daarbij ook de rol om toe te zien dat vernieuwingen geen of minimale privacy risico's met zich mee brengen (privacy by Design). DRD werkt voor (interne) afnemers en medewerkers hebben de awareness om privacy risico's te mitigeren. Bijvoorbeeld als meer data worden geleverd dan nodig is voor een onderzoek, dan zal een DRD medewerker sturen op data minimalisatie.

In het kader van de Wet Bescherming Persoonsgegevens (WBP) dienen bestanden die privacy gevoelige gegevens van personen en bedrijven bevatten geregistreerd te worden. In de documenten op het Intranet [Wet Bescherming Persoonsgegevens](#), staat informatie over hoe met bestanden die gevoelige gegevens bevatten dient te worden omgegaan. De registratie van deze bestanden gebeurt in het excelbestand "BPM verzamelstaat gebruik microdata.xlsx".

Bij DRD kan in projectverband of voor een adviesopdracht met versleutelde (verrind) microdatasets worden gewerkt. BSN nummers worden in principe niet binnen DRD gebruikt. DRD streeft ernaar zo min mogelijk datasets in de eigen mappen beschikbaar te stellen. Voor projecten en adviesopdrachten wordt zo veel als mogelijk (tijdelijk) gebruik gemaakt van de data in de mappen die bij de statistische afdeling beschikbaar zijn en benodigd is voor het betreffende project/onderzoek. Het beperken van toegang tot dergelijke persoonsgegevens blijft de verantwoordelijkheid van statistiekafdelingen. De microdatasets bevatten vaak zeer veel kenmerken. Slim combineren van microbestanden kan toch tot situaties leiden waarbij privacy in het geding komt. Dat is niet volledig uit te bannen. Dergelijke informatie blijft wel begrensd beschikbaar binnen het project bij een beperkte groep medewerkers, die zich bewust zijn van privacybescherming. Dergelijke projecten worden binnen een afgeschermd, van de buitenwereld afgesloten "SEC-omgeving" uitgevoerd, waarbij de toegang tot bestanden alleen mogelijk is voor een beperkte groep medewerkers met een SEC-account. De geheimhouding clause die elke CBS medewerker tekent dekt afdoende af dat hier verder geen misbruik zal ontstaan. Dat laatste geldt ook voor tijdelijke krachten. DRD werkt inhoudelijk veel samen met universiteiten, waarbij veel PhD's of studenten worden betrokken bij onderzoeken. Die doorlopen vanuit een bijzondere constructie dezelfde aanstellingsprocedure als vaste CBS medewerkers binnen DRD, inclusief de toezegging om zorgvuldig om te gaan met informatie.

Bij de samenwerking met hoogleraren is de awareness en privacy borging geregeld via de universiteiten.

Rechten op mappen binnen een project gelden voor een begrensde periode. Ook zijn gegevens vaak maar tijdelijk beschikbaar. Opschoning van de genoemde (rechten op) mappen en accounts op de SEC-omgeving is een aandachtspunt. Daarbij speelt ook dat vanuit methodologisch oogpunt lange tijdreeksen juist cruciaal zijn voor het onderzoeken van ontwikkelingen, maar ook om over langere periodes cijfermatige inzichten te kunnen opleveren.



Voor een overzicht van specifieke privacy gevoeligheden en noodzakelijke beheersmaatregelen binnen DRD wordt verwezen naar bijlage 3.

DBD

Binnen Beleidsstatistieken, Dataservices en Remote Access is veel aandacht voor privacybescherming en informatiebeveiliging. Dit heeft DBD goed op orde en waar mogelijk wordt hier vanuit ontwikkeltrajecten gewerkt aan verbetering. O.a. afhankelijk van aanvullend beschikbaar gestelde middelen.

DBD werkt zo veel mogelijk in een (zogenoemde SEC-)omgeving waarbij de data zijn verrind. Data die DBD ontvangt van externe partijen wordt bij binnenkomst direct aan het organisatieonderdeel dat het verrinnen uitvoert aangeboden en daarna verwijderd.

DBD legt contractueel vast wanneer data van externen wordt vernietigd en hoe met data wordt omgegaan.

DBD voert het project 'kwaliteit stelsel basisregistraties' uit waarbij BSN tot op het laatst bewaard moet blijven. Daartoe is een aparte werkomgeving ingericht waarvoor alleen specifieke projectmedewerkers rechten hebben. Deze rechten worden ingetrokken op het moment dat het project is afgelopen of mensen het project verlaten. Op dit moment hebben vier personen rechten om op die omgeving te werken.

Met betrekking tot privacy en dataminimalisatie heeft DBD naar aanleiding van eerder gestelde vragen over privacy een aantal beheersmaatregelen genomen (zie bijlage 4).

Bijlage 1: Bewaartermijnen DVZ mbt primaire waarneming

- 1x per jaar – medio van dat jaar – expliciet kijken naar het bewaren en vernietigen en dus het '**proces van bewaren en vernietigen**' uit te voeren. Voor sommige type gegevens moet dit frequenter - in de 'dagelijkse gang van zaken' inbedden. Het is dan aan de betreffende proceseigenaar om te bepalen wanneer/hoe vaak.
- **Vernietigen vanuit functionaliteit in systemen:** om gegevens van enquêtes te vernietigen o.b.v. verslagjaar of specifieke enquêtebestanden die eerder vernietigd kunnen worden - impactanalyse gereed en op roadmap 2021 - gegevens van eenheid binnen onderzoek - gegevens van eenheid - algemene gegevens onderzoek - gegevens van interviewers - voorlopige versies van ontwerpproducten - logistieke testdata en testresultaten - vragenlijstjablonen en benaderproductsjablonen - gegevens tbv analyses (van M&A) en (technische) logging.

De drie DVZ agile teams zullen moeten gaan kijken hoe ze e.e.a. gaan vormgeven.

- **Bewaren van documenten – archivering** t.b.v. de reproduceerbaarheid, om achteraf aan te tonen wat we als DVZ – op hoofdlijn – gedaan hebben qua onderzoeken - specifieke procedure nodig voor Onderzoeksdesign, vragenlijstontwerp, steekproefontwerp, enquêteverantwoording en jaarplanning. Daarnaast ook – als uitzondering – de Doodsoorzakenformulieren. Overdracht aan Nationaal Archief o.b.v. CBS-breed proces – aanhaken bij nieuwe archiefwet waarbij het CBS zaken zelf mag bewaren. Hoe en wat?



- Er is ook procedureel, **handmatig werk** nodig voor veilig stellen van te bewaren documenten en voor vernietigen van diverse typen documenten en bestanden (zoals plannings, verslagen, notulen, etc). De proceseigenaar is verantwoordelijk en zal met medewerkers gaan kijken hoe dit vorm te geven.
- **Vastleggen** wat, wanneer bewaard en vernietigd is en door wie - verantwoordelijkheid van de proceseigenaar – via **proces verbalen**, CBS-breed issue.
- Achterstand qua bewaren en vernietigen – **inhaalslag** (exceptie) – bij FG formeel melden dat er een achterstand is en aan te geven wanneer we de achterstand inhalen.
- Bovenstaande per 1-1-2022 **effectueren** – per medio 2022 voor de eerste keer een grote actie om zaken te gaan veiligstellen en te gaan vernietigen.

Bijlage 2: Beheersmaatregelen binnen DVZ om privacy beter te beschermen

- **Verwerkersovereenkomsten**
Waar data verzamelen gebruik maakt van derde partijen, die deelproducten opleveren ten behoeve van het proces van data verzamelen, zijn verwerkersovereenkomsten afgesloten als persoonsgegevens in het geding zijn. Deze overeenkomsten borgen dat de toeleverancier voldoende toeziet op privacy borging. Binnen DRI wordt een overzicht bijgehouden van dergelijke partijen en bijbehorende verwerkersovereenkomsten.
- **Telefoonnummerverrijking**
Daartoe worden telefoonnummers van marktpartijen gebruikt (tegen betaling) om CATI in staat te stellen om respondenten telefonisch te benaderen. Hieraan zijn privacy risico's verbonden. Eigenaren van telefoonnummers kunnen vragen hoe men aan hun telefoonnummer komt, als zij hier niet expliciet toestemming voor hebben gegeven. Beheersmaatregelen hierbij zijn: zoeken naar leveranciers van telefoonnummers waarbij gebruik door het CBS juridisch zodanig vastligt dat privacy schending niet aan de orde is of nog beter, de CBS-wet zodanig aanpassen (in analogie met andere EU landen) dat het CBS rechtstreeks telefoonbestanden mag opvragen bij telecomaانبieders ten behoeve van statistiek maken. Bij het inrichten van een tijdelijk alternatief proces totdat wetgeving is aangepast, wordt kritisch gekeken of juridische en privacy kaders afdoende worden nagekomen vanuit proportionaliteit en subsidiariteitsprincipes. Waar nodig wordt een PIA opgesteld en worden beheersmaatregelen ingebed in het proces.
- **Geautomatiseerd vastleggen van gewerkte uren en verreden kilometers**
Voor de geautomatiseerde vastlegging van gewerkte uren en gereden kilometers door interviewers binnen CAPI wordt gebruik gemaakt van de W2C tooling (derde partij). Deze tooling registreert privacygevoelige informatie van eigen medewerkers in de vorm van locatie en werktijden. Bij de keuze en implementatie van deze tool is kritisch gekeken naar hoe privacy breeches worden voorkomen. Daarbij is een PIA opgesteld en zijn beheersmaatregelen in het proces opgenomen. Dat betreft o.a. gevoelige informatie (locatie) zo kort mogelijk vasthouden zodanig dat niet te traceren is waar iemand zich op enig moment ophoudt. Ook is in de processen geregeld dat zo min mogelijk gevoelige informatie wordt opgeslagen. Waar mogelijk gebeurt dat door data zo snel mogelijk te anonimiseren en terug te brengen tot informatie die niet anders is dan wat in weekstaten en reisdeclaraties al sinds jaar en dag wordt ingevuld.



- **Secundaire bronnen**

DVZ is de plek waar secundaire bronnen in de vorm van databestanden vanuit up- en download via beveiligde protocollen het CBS binnen komen. Deze bestanden worden direct en geautomatiseerd doorgezet naar de statistiekafdelingen. Deze bestanden worden maximaal 6 weken bewaard, zodat nalevering mogelijk als statistiek afdelingen daarom vragen. Geleverde bestanden worden bewaard in een specifieke map met beperkte toegankelijkheid. Medewerkers die hier toegang toe hebben zijn gebonden aan geheimhouding. Daar waar statistiekafdelingen nog via informele wegen gegevens binnen krijgen, is het de verantwoordelijkheid van de statistiekafdelingen om privacy borging af te hechten.

DVZ bewaart ook gegevens van toeleveranciers van bronnen. Dit betreft de minimale informatie die nodig is om deze leveranciers te kunnen communiceren en zijn door de leveranciers zelf aangeleverd.

- **Logistieke proces rondom benaderproducten**

Binnen het logistieke proces rondom uitzendingen zijn persoonsgegevens nodig voor het kunnen versturen van brieven, benaderproducten en incentives. De privacy borging hierbij is de verantwoordelijkheid van BFB.

- **Achtergrondkenmerken in de benaderstrategie.**

Het komt voor dat persoonsgegevens die het CBS al verzameld heeft gebruikt worden in het waarneemproces voor nieuw uit te vragen gegevens, als achtergrondkenmerken in de benaderstrategie. Met als doel een zo goed mogelijke kwaliteit van de statistische output te verkrijgen. Het gaat hier veelal om algemene persoonskenmerken die als onderscheidende kenmerken worden meegenomen in de steekproef of de benadering van te enquêteren personen. Er wordt dus bij de waarneming op basis van reeds verzamelde persoonsgegevens gedifferentieerd naar persoonskenmerken om aan statistische informatie te komen. Op dit moment wordt beschreven hoe dit gebeurt binnen de privacy kaders.

- **Toegang tot gegevens binnen DVZ**

Toegang tot gegevens, maakt niet uit of deze in een map of database staan, wordt geregeld m.b.v. Varonis. Dat gebeurt binnen Phoenix op basis van toegangsrechten tot een bepaalde applicatie vanuit een rol (role based access). Applicaties van Phoenix (o.a. COM, DataToegang en Onderzoeks Ontwerp) maken gebruik van relationele databases om data te verwerken. Afhankelijk van de rol die je in de DVZ organisatie hebt, kun je met Phoenix meer of minder functionaliteit en afgeleid daarvan data benaderen. Hiertoe wordt je lid gemaakt van de juiste Varonis-Phoenix-rolgroep. Voor DataToegang is de afscherming niet meer geregeld via mappen, maar via "datacontracten" (een stuk software net als Varonis). Via codes is er toegang tot de software van datacontracten, waarbij privacy borging (wie heeft toegang tot welke data) helemaal is geregeld. Bij bijv. Datatoegang (applicatie) is toegang mogelijk tot alle waargenomen data, maar een medewerker van het Budgetonderzoek kan niet bij een ander onderzoek komen.

Omdat meerdere proceseigenaren gebruik maken van deze applicaties, moet verantwoordelijkheid voor wie hier structureel op toeziet nog opnieuw binnen DVZ worden ingevuld. Momenteel is de projectleider nog degene die toeziet wie wel of geen rechten op de data van een onderzoek in datatoegang krijgt. In audits kan worden getoetst op



continuïteit in het actualiseren van datatoegang. Er is een agile team dat de applicatie Datatoegang beheerd.

In de MS2014 methodiek geeft elk van de vier standaard gedefinieerde rolgroepen een andere combinatie van toegang tot de vier standaard gedefinieerde submappen van een share. Dat voedt de behoefte van de CIO voor inzicht in welke medewerkers toegang hebben tot welke MS2014 mappen. Binnen de Phoenix aanpak is dat helemaal geen issue, en daarmee is de borging van privacy daar beter gefaciliteerd.

- **Wachtwoordbeleid**

voor respondenten is compliant indien 2 factor authenticatie is ingeregeld (m.b.t. bijzondere persoonsgegevens, zoals bijvoorbeeld gezondheidsdata in enquêtes). Dit speelt voor primaire waarneming. Let op 2 factor authenticatie in de buitenwereld betekent aan de ene kant autorisatie hebben, waarna nog getoetst wordt of je wel de persoon bent die de autorisatie heeft. Denk aan DIGID waar je inlogt waarna je nog een code via SMS moet insturen. Of waarbij je een QR code laat zien, waarna je nog een legitimatie moet laten zien. Binnen het CBS wordt hier over 2 factor authenticatie gesproken als de gebruikersnaam en wachtwoord apart via verschillende media worden verstuurd. Dat is feitelijk een andere definitie / invulling. Daarnaast is er een project voor een sterk wachtwoord beleid. PL per onderzoek weet binnen DVZ hoe dit voor elk onderzoek is geregeld. *Hoe en wat meer specifiek uitvragen bij* 5.1.2.e *en* 5.1.2.e

5.1.2.e

Voor secundaire waarneming is 2 factor authenticatie alleen nodig bij Download omdat het specifieke bedrijfsgegevens betreft. Bij upload is dit niet aan orde. In nieuwe Phoenix systemen worden gebruikersnaam en wachtwoord gescheiden verstuurd.

Bijlage 3: Beheersmaatregelen binnen DRD om privacy beter te beschermen

- **Privacy risico gegevens PHDs en studenten door decentralisatie van administratief werk**
Zoals al benoemd heeft DRD te maken met een relatief grote doorloop van medewerkers a.g.v. samenwerking met PhD's en studenten. Omdat deze medewerkers dezelfde procedures doorlopen als bij de aanstelling van vaste medewerkers, gelden daarvoor ook dezelfde HR procedures, inclusief identificatie en het beschikbaar stellen van de juiste persoonsgegevens. In het nieuwe Casper systeem is dit gedecentraliseerd en is het de taak van de manager deze informatie vast te leggen. Bij veel verloop is dat veel werk. Daarbij wordt veel informatie uitgewisseld op verschillende manieren, waarbij ook gegevens (tijdelijk) worden opgeslagen. Denk aan kopie van paspoort. De vraag is of binnen het CBS afdoende wordt gefaciliteerd dat verantwoordelijke teamhoofden hier de noodzakelijke borging kunnen garanderen. In situaties waar teamhoofden niet de tijd vinden om dergelijke informatie weer tijdig op te ruimen, zorgt decentralisatie voor extra privacy risico's m.b.t. persoonsgegevens van de eigen medewerkers.

Een andere vraag is of decentralisatie vanuit Casper bijdraagt aan meer privacy risico's bij het correct vullen van het bedrijfsvoeringsysteem, bijvoorbeeld bij het inkoopproces? Degene die informatie moet invoeren, vraagt benodigde informatie uit bij toeleveranciers of zoals hiervoor benoemd bij nieuwe medewerkers of Als e-mails, andere bestanden



etc niet worden opgeruimd dan ontstaat een grotere kans op misbruik van die gegevens. De vraag is of de impact zodanig is dat hier extra maatregelen voor moeten worden genomen.

Bijlage 4: Beheersmaatregelen binnen DBD om privacy beter te beschermen

- **Actualisatie van procesbeschrijvingen**
Vanuit de privacy audits zijn enkele bevindingen naar voren gekomen vooral in relatie tot actuele procesbeschrijvingen, die vaak (te) laat worden geactualiseerd naar nieuwe situaties. Vooral bij personele wisselingen.
- **Communicatie van privacy beleid en beheersmaatregelen**
Privacy en gegevens beveiliging is technisch goed geregeld en gedocumenteerd, maar niet op een zodanige wijze dat dit met de buitenwereld kan worden gedeeld. Het op een begrijpbare manier aan buitenstaanders (het publiek) uitleggen wat het beleid is van het CBS m.b.t. privacy en welke maatregelen worden genomen om gegevens te beschermen, is een belangrijk verbeterpunt.
- **Verwerkersovereenkomsten**
Waar DBD gebruik maakt van derde partijen, die deelproducten opleveren ten behoeve van het proces van beleidsstatistieken, dataservices of remote access, zijn verwerkersovereenkomsten afgesloten als privacy in het geding is. Deze overeenkomsten borgen dat de toeleverancier voldoende toeziet op privacy borging. Binnen DRI wordt een overzicht bijgehouden van dergelijke partijen en verwerkersovereenkomsten.
- **Bewaartermijnen**
 - Onverrindde bestanden Beleidsstatistiek
Gegevens voor Beleidsstatistieken worden bij binnenkomst verrind door CBK. De initiële data wordt vervolgens verwijderd. De termijn waarop dit gebeurt verschilt. Daartoe zijn richtlijnen opgesteld en meegenomen in een update van de Richtlijnen voor onderzoekers.
 - Onverrindde bestanden DVZ
Voor DBD kunnen bewaartermijnen beperkt worden, maar daarop sturen loopt aan tegen CBS afspraken dat gegevens 2,5 jaar bewaard worden. Alternatief is dan om gegevens handmatig te verwijderen. Met DVZ is afgestemd om de bewaartermijn voor deze specifieke bestanden op 1 maand te zetten.
 - Bestanden BSUP (uploadkanaal Beleidsstatistiek)
Hiervoor bestaat geen richtlijn voor de bewaartermijn. De BSUP map wordt meenemen in de halfjaarlijkse opschoonactie.
 - Onverrindde bestanden overige afdelingen
Om te voorkomen dat dat bestanden in de niet-SEC omgeving afkomstig van andere afdelingen in hun inputmappen blijft staan, maakt de projectleider de afspraak met inhoudelijke afdelingen over de termijn waarop bestanden worden verwijderd. Na de afgesproken tijd vraagt de projectleider een bevestiging van vernietiging bij de betreffende afdeling. Ook dat is opgenomen in de update van de Richtlijnen.
- **Aanlevering onverrindde data**
In de update van de Richtlijn is opgenomen dat onverrindde data altijd wordt aangeleverd via het uploadkanaal.



- **Onverrinde data in projecten**

De projectmappen van projecten waarin met onverrinde data wordt gewerkt (specifiek: projecten Basisregistratie en Leegstand) worden beter beveiligd, zodat deze niet toegankelijk zijn voor de hele afdeling. Er is een nieuwe werkomgeving ingericht voor deze projecten. Op dit moment wordt aan de 'kwaliteitsmeting stelsel basisregistraties' gewerkt en vier personen hebben rechten op deze werkomgeving. Mappen enkel openstellen voor de onderzoekers op het project. Het management van DBD ziet hier verder op toe.

- **Onverrinde data over gebouwen**

Adressen met ruimtelijke of gebouwkenmerken zijn op zich niet gevoelig (anders als BSN's en KVK's). Wanneer deze gegevens echter gecombineerd worden met informatie over personen zijn deze gegevens wel gevoelig. Adressen aan sich vallen niet onder de AVG-wet. Wel wil het CBS niet dat deze zomaar op straat komen te liggen. Niet alle afdelingen zijn zo ver om ook adressen te anonimiseren en plausibiliteitscontroles worden ook vaak op objectniveau gedaan. Maar net zoals bij Vastgoed en Wonen wordt hier steeds kritisch naar gekeken en waar mogelijk gewerkt met versleutelde gegevens.

- **Onverrinde KVK-nummers**

Niet-natuurlijke personen vallen niet onder de AVG-wet. De privacy van bedrijven is echter ook belangrijk voor het CBS. Er worden bij de economische afdelingen al acties tot 'verbrinnen' ingezet. Wel zijn ze niet zo ver dat het altijd mogelijk is om met versleutelde KVK's te werken. Binnen CvB werken we met versleutelde gegevens waar het even kan en blijven kritisch en met elkaar in overleg.

- **Beperken netwerkcapaciteit Beleidsstatistieken**

Beleidsstatistiek produceert veel bestanden die een grote belasting vormen voor het netwerk. Er worden veel tussenbestanden opgeslagen en veel onnodige variabelen in bestanden. Dat levert problemen met de opslagcapaciteit, is foutgevoelig en tijdrovend. De werkwijze omtrent het plaatsen van bestanden wordt aangepast op basis van een nieuw startsjabloon syntax/syntaxenplan.

- **Bronbestanden POMO-project**

In het verleden werden aangeleverde, niet-verrind bestanden in de SEC-omgeving geplaatst. Voor het POMO-project is gevraagd bronbestanden niet te verwijderen vanwege ingewikkelde materie en noodzaak zaken te kunnen reproduceren ten behoeve van herhaalmetingen. In principe moet alleen het dataframe worden behouden. Bronbestanden zijn inmiddels verwijderd. Het P-direct bestand met Rin nummers in de datamap gebruikt hetzelfde format en daarom is zelfs het dataframe overbodig.

- **Leegstandproject**

Bestanden worden onverrind aangeleverd omdat werken in het SSB veel vertraging oplevert en omdat het mogelijk moet zijn gebouwen te checken op bepaalde kenmerken (gebruiksfunctie en leegstand). Bij het opvragen van het BRP bestand van de afdeling demografie zijn BSN's niet noodzakelijk en is het afdoende om deze te vervangen door een 1 voor bewoond. Deze nieuwe werkwijze kan gebruikt worden in de update van het leegstand project.

BSNs worden dit jaar in de eerste stap verwijderd en komen dus enkel voor in de bronbestanden. Voor volgend jaar wordt de nieuwe werkwijze afgestemd met team Demografie. Er wordt dan geen BSN data meer ontvangen.