Privacybeleid CBS

Inhoudsopgave

1. Inleiding

De bescherming van gegevens is voor het CBS topprioriteit. Het Privacybeleid beschrijft de kaders en uitgangspunten van het CBS als het gaat om het beschermen van alle gegevens die het CBS verwerkt. De samenleving moet erop kunnen vertrouwen dat alle gegevens die het CBS ontvangt, uitsluitend gebruikt worden voor het vervaardigen van statistiek en dat dit nooit leidt tot onthulling van informatie over individuele personen, huishoudens, ondernemingen of instellingen. De Wet op het Centraal Bureau voor de Statistiek (Wet CBS) stelt het CBS verplicht om zorg te dragen voor 'de nodige technische en organisatorische voorzieningen ter beveiliging van zijn gegevens tegen verlies of aantasting en tegen onbevoegde kennisneming, wijziging en verstrekking van die gegevens (artikel 38 Wet CBS)'. De Wet CBS ziet dus niet alleen op gegevens van personen en huishoudens, maar ook op ondernemingen en instellingen. De Wet CBS heeft hiermee een grotere reikwijdte dan de Algemene Verordening Gegevensbescherming (AVG) die zich beperkt tot het beschermen van persoonsgegevens. Het Privacybeleid van het CBS omvat daarom de bescherming van alle gegevens die het CBS ontvangt in. Het CBS wil niet alleen voldoen aan wetgeving op het gebied van privacy, maar heeft ook de ambitie om te excelleren.

Het CBS heeft een breed palet aan technische en organisatorische maatregelen om privacy optimaal in de organisatie te borgen en hier aandacht aan te blijven besteden. Privacybescherming is namelijk nooit af. Het is een dynamisch proces dat het hoofd moet bieden aan toenemende dreigingen, onder meer op het gebied van cybercrime, en zich aan moet passen aan veranderende maatschappelijke inzichten, technologische ontwikkelingen en gewijzigde wet- en regelgeving. Het Privacybeleid van het CBS bevat daarom geen opsomming van maatregelen, maar juist de uitgangspunten en kaders die gehanteerd worden bij processen van alle gegevens die het CBS verwerkt.

Het doel van het Privacybeleid van het CBS is om duidelijkheid te verschaffen over de wijze van bescherming van de gegevens die door de samenleving aan het CBS worden verstrekt. Alleen wanneer het CBS de belangen van betrokkenen volledig beschermt en vertrouwen geniet vanuit de samenleving, de 'social license' behoudt, kan het CBS zijn wettelijke taak blijven uitoefenen in de toekomst. Dit Privacybeleid is voor intern en extern gebruik.

2. Missie CBS en privacybescherming

De missie van het CBS is het samenstellen en publiceren van betrouwbare en samenhangende statistische informatie die inspeelt op de behoefte van de samenleving. Alles wat het CBS doet staat in het teken van deze missie en de daarvan afgeleide kernwaarden: betrouwbaar, objectief en maatschappijgericht. De missie en positie van het CBS zijn afgeleid van de Wet CBS. De wet biedt het CBS veel mogelijkheden voor het verwerken van gegevens, maar ook de plicht om de gegevens op een veilige wijze te verwerken en te beschermen. Het Privacybeleid draagt op deze wijze bij aan de missie van het CBS en aan het voldoen aan wet en regelgeving ten aanzien van de Wet CBS en de AVG.

2.1 Scope

Het CBS heeft de bescherming van gegevens hoog in het vaandel staan. Het CBS heeft de taak om de enorme hoeveelheid informatie die het over individuele personen, huishoudens, ondernemingen en instellingen ontvangt, veilig te verwerken en ervoor te zorgen er geen herleidbare informatie wordt onthuld.

De scope van dit Privacybeleid betreft:

1. gegevens ten behoeve van statistisch onderzoek t.b.v. de wettelijke taak van het CBS:
   a) gegevens over personen en huishoudens;
   b) gegevens over ondernemingen en instellingen.
2. gegevens ten behoeve van bedrijfsprocessen.
   Dit betreffen gegevens over het eigen personeel of ten behoeve van de bedrijfsvoering. Voor verwerkingen met gegevens van het eigen personeel, bijvoorbeeld medewerkerstevredenheidsonderzoek of monitoring, geldt een andere grondslag en doelbinding dan voor statistische verwerkingen ten behoeve van de wettelijke taak van het CBS. Om deze reden wordt deze categorie apart genoemd. Ook gegevens van burgers die verzoeken indienen (zoals WOO verzoeken, informatieverzoeken en klachten) vallen onder bedrijfsprocessen.

Wat zijn persoonsgegevens?
De AVG (artikel 4) definieert een persoonsgegeven als: “alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon (de betrokkene)”. Als identificeerbaar wordt beschouwd: “een natuurlijke persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identificator zoals een naam, een identificatienummer, locatiegegevens, een online identificator of van een of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon”.

Bijzondere categorieën persoonsgegevens, strafrechtgegevens en Burgersurvicenummers?
Bijzondere categorieën persoonsgegevens genieten extra bescherming in de AVG omdat verwerking van deze gegevens grote impact op iemand kan hebben. Het gaat bijvoorbeeld om etnische afkomst, religieuze overtuigingen of gezondheidsgegevens (zie Bijlage 2 Definities). Strafrechtelijke gegevens en het Burgerservicenummer (BSN) vallen niet onder de bijzondere categorieën persoonsgegevens maar ook voor deze gegevens zitten voorwaarden voor gebruik vanuit de AVG (artikel 9, 10 en 87 van de AVG). Het CBS is middels de Wet CBS gerechtigd al deze gegevens te gebruiken.

Wat zijn bedrijfsgegevens?
Het CBS werkt ook met gegevens over ondernemingen en instellingen, de bedrijfsgegevens. Er is niet altijd een duidelijke scheidslijn tussen persoons- en bedrijfsgegevens. Zo hebben eenmanszaken, vennootschap onder firma (vof) en ZZP’ers geen rechtspersoonlijkheid in de zin van boek 2 Burgerlijk Wetboek. De natuurlijk persoon achter de onderneming is vaak herkenbaar waardoor eigenschappen van de onderneming al snel als eigenschappen van een natuurlijk persoon en dus als persoonsgegevens in de zin van de AVG moeten worden gezien.

Voor persoons-en bedrijfsgegevens gelden verschillende processen. Zo is het voor een statistiek nooit relevant om een individu te kunnen herkennen. Daarom worden persoonsgegevens zo snel mogelijk na binnenkomst bij het CBS gepseudonimiseerd. Bij bedrijfsgegevens is het voor het statistisch proces vaak wel relevant te weten om welk individueel bedrijf het gaat. Om die reden vind pseudonimisering vaak in een later stadium plaats.

2.2 De beginselen van de AVG

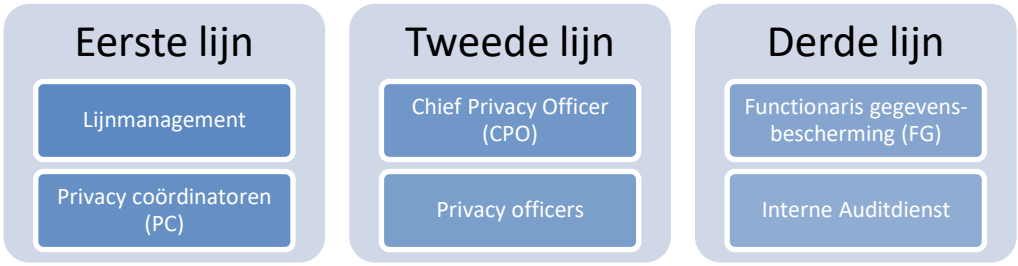
Artikel 5 lid 1a tot en met f van de AVG beschrijft de beginselen die het CBS als verwerkingsverantwoordelijke verplicht moet naleven bij het verwerken van persoonsgegevens. Het CBS is altijd verwerkingsverantwoordelijke en geen verwerker omdat het CBS zelf het doel en de middelen bepaalt. Een verwerker verwerkt alleen persoonsgegevens in opdracht van anderen. Daar is bij het CBS nooit sprake van.
De beginselen zijn:

a) rechtmatigheid, behoorlijkheid en transparantie;
b) doelbinding;
c) minimale gegevensverwerking;
d) juistheid;
e) opslagbeperking;
f) integriteit en vertrouwelijkheid.

Artikel 5 lid 2 van de AVG verplicht het CBS tot naleving van bovenstaande beginselen en moet dit ook kunnen aantonen (verantwoordingsplicht). In hoofdstuk 3 worden de beginselen verder toegelicht.

2.3 Privacy governance: het three lines model

Door toenemende digitalisering, en daarmee de toenemende hoeveelheid aan gegevens, en grotere cybersecurityrisico's is gegevensbescherming complexer geworden. Om beleid, overzicht en coördinatie van privacybescherming beter te borgen in de organisatie, hanteert het CBS sinds 2021 het model van 'three lines', in navolging van het Ministerie Economische Zaken en Klimaat (EZK).



Eerste lijn

In dit model is het lijnmanagement als 'eerste lijn' verantwoordelijk voor de strategische visie en het borgen van de aantoonbare naleving van de wet- en regelgeving op het terrein van privacybescherming en de risicobeheersing van die naleving. Privacycoördinatoren vervullen hier een adviserende en coördinerende rol ten behoeve van het lijnmanagement en maken dus een onderdeel uit van de eerste lijn.

Iedere hoofddirectie beschikt over tenminste één privacycoördinator. Deze coördinator vertaalt het CBS-brede Privacybeleid naar de hoofddirectie en werkt daarbij nauw samen met de andere privacycoördinatoren, de Chief Privacy Officer (CPO), de Functionaris Gegevensbescherming (FG) en de privacy officers. De privacycoördinator ondersteunt het management bij de dagelijkse afhandeling van privacy aangelegenheden voor de hoofddirectie en fungeert als vraagbaak voor het lijnmanagement ten aanzien van privacyvraagstukken.

Tweede lijn

Als 'tweede lijn' opereren de CPO en de privacy officers. De CPO is belast met de concernbrede advisering en aanpak van privacybescherming. De CPO zoekt naar de privacy knelpunten en behoeftes die spelen in het CBS en inventariseert best practices bij de verschillende directies. De CPO gebruikt de aanbevelingen van de FG, de privacy officers en interne en externe audits om te komen tot verbetering van de beleidskaders. De CPO voert deze taak uit in nauwe afstemming met de privacy coördinatoren, privacy officers en de FG. Ook overlegt de CPO met de Chief Information Security Officer (CISO) en de Chief Quality Officer (CQO) voor gezamenlijk beleid en advies op het gebied van kwaliteit, informatiebeveiliging en privacybescherming. De

CPO sluit aan bij het interdepartementale CPO netwerk en is aanspreekpunt voor externe relaties bij privacyvraagstukken. De CPO rapporteert periodiek aan het DB.

De privacy officers van team CSB-Juridisch, spelen een belangrijke rol bij de naleving van wet- en regelgeving. Zij adviseren gevraagd en ongevraagd over alle juridische aspecten van privacywetgeving en zorgen samen met CPO en de FG ook voor juridische kennisdeling binnen het CBS.

Derde lijn

De derde lijn wordt ingevuld door de interne auditdienst en de FG als 'interne toezichthouders' van het CBS. De FG is de interne toezichthouder op de bescherming van persoonsgegevens en – in het geval van het CBS – ook van bedrijfsgegevens. De FG geeft gevraagd en ongevraagd advies over verwerkingen van persoonsgegevens en over beleid dat daarmee te maken heeft. Bovendien legt de FG uit hoe de AVG moet worden geïnterpreteerd. De FG rapporteert rechtstreeks aan de Directeur Generaal (DG) van het CBS in een maandelijks overleg.

De interne auditdienst focust zich op kwaliteitsmanagement, privacybescherming en informatiebeveiliging. Op alle drie de aandachtsgebieden wordt (in samenhang) gestreefd naar aantoonbare compliance met algemeen erkende, externe (inter)nationale normenkaders en wetgeving (ISO 9001, ISO 279001, de AVG en NOREA). Hierop worden interne audits uitgevoerd. Het CBS laat daarnaast jaarlijks externe audits uitvoeren op deze drie terreinen waarbij het certificatieproces wordt begeleid door de interne auditdienst. De interne en externe audits helpen het CBS naar het continu verbeteren van de eigen processen als zelflerende organisatie.

3. CBS brede privacymaatregelen

Het CBS is volgens artikel 25 van de AVG verplicht adequate technische en organisatorische maatregelen te nemen die redelijkerwijs verwacht kunnen worden om aan de AVG beginselen te voldoen. Daarbij moet rekening gehouden worden met de stand van de techniek, de uitvoeringskosten, en de aard, de omvang, de context en het doel van de verwerking. Dit moet afgewogen worden tegen de risico's voor de betrokkenen. Vanuit de Wet CBS (artikel 38) geldt dezelfde verplichting tot bescherming van álle gegevens die het CBS verwerkt.

De beginselen van de AVG vormen het uitgangspunt voor het CBS brede Privacybeleid. In dit hoofdstuk wordt eerst, aan de hand van de beginselen zelf, toegelicht wat dit betekent voor het CBS. Daarbij is vooral aandacht voor de eerste twee beginselen, a) rechtmatigheid, behoorlijkheid en transparantie, en b) doelbinding. De overige beginselen worden kort toegelicht en komen uitgebreider aan bod in hoofdstuk 4 Privacy by Design. Aan het einde van dit hoofdstuk wordt een aantal voorbeelden gegeven van generieke privacymaatregelen van het CBS.

3.1 Beginsel a) van de AVG: rechtmatigheid, behoorlijkheid en transparantie

Een verwerking moet altijd rechtmatig zijn, oftewel, organisaties mogen persoonsgegevens alleen verwerken in overeenstemming met de wet. Voor betrokkenen moet het behoorlijk en transparant zijn hoe en waarom hun persoonsgegevens verwerkt worden. Zij hebben recht op informatie over welke organisaties hun gegevens verwerkt en voor welk doel. De doelbinding komt uitgebreider aan bod bij beginsel b.

Artikel 6 lid 1 van de AVG noemt zes grondslagen. Een verwerking moet altijd aan één van deze grondslagen voldoen om rechtmatig te zijn:

a. toestemming. Toestemming moet vrijelijk worden gegeven. Dat is lastig als er sprake is van een machtsverhouding (overheid-burger of werkgever-werknemer). Toestemming moet ook ondubbelzinnig zijn, een duidelijke actieve handeling om toestemming te geven (bijvoorbeeld een schriftelijke verklaring). Tenslotte moet toestemming geïnformeerd en specifiek zijn (wie verzamelt wat met welke doelbinding) en moet ook eenvoudig ingetrokken kunnen worden. Vooral bedrijven maken vaak gebruik van deze grondslag. Bijvoorbeeld bij een online aankoop wordt expliciet toestemming gevraagd om nieuwsbrieven te mogen versturen naar het opgegeven mailadres;
b. uitvoeren van een overeenkomst. Deze grondslag wordt gebruikt als de verwerking nodig is om de overeenkomst uit te voeren. Iemand koopt bijvoorbeeld online een product, de verkoper heeft dan adresgegevens nodig om dat product op te kunnen sturen. Wil de verkoper daarnaast ook nieuwsbrieven versturen, dan is daarvoor weer toestemming nodig. Dit laatste is dus een aparte grondslag, daar mag niet dezelfde grondslag voor gebruikt worden;
c. wettelijke verplichting. Deze grondslag wordt alleen gebruikt wanneer een verwerking noodzakelijk is om aan een wettelijke verplichting te voldoen. Een voorbeeld is de wettelijke verplichting van werkgevers om loongegevens van werknemers te verstrekken aan de belastingdienst. Deze grondslag mag niet worden gebruikt wanneer een (overheids)organisatie een taak van algemeen belang uitoefent. Daarvoor is grondslag e) voor bedoeld;
d. beschermen vitale belangen. Een vitaal belang komt alleen voor als het essentieel is voor iemands leven of gezondheid, bijvoorbeeld bij acuut gevaar. Als iemand bewusteloos is kan er niet om toestemming gevraagd worden;
e. taak van algemeen belang of openbaar gezag. Deze grondslag is voor het CBS van toepassing voor alle statistische verwerkingen die het CBS uitvoert in het kader van de Wet CBS. De verwerking is noodzakelijk voor de vervulling van een taak van algemeen belang dat aan de verwerkingsverantwoordelijke is opgedragen (bij wet aangewezen). Het gaat daarbij om taken die in de wet zijn vastgelegd en die relevant zijn voor de betreffende

organisatie. Het CBS is middels de Wet CBS aangewezen voor een taak van algemeen belang;

f. gerechtvaardigd belang. Deze grondslag mag alleen gebruikt worden als het belang ergens in het recht is opgenomen, wordt erkend en beschermd. Dat mag ook in een ongeschreven rechtsregel of rechtsbeginsel zijn. Als het maar gaat om een belang waarvan we in de maatschappij vinden dat het door het recht beschermd moet worden. De verwerking is noodzakelijk om dit belang te behartigen en er is een afweging gemaakt tussen het belang voor de organisatie en het belang van de betrokkenen. Verwerkingen die bijdragen aan goed werkgeverschap worden vaak onder deze grondslag geschaard (verplichtingen die op een bedrijf of instelling rusten op basis van bijvoorbeeld het Burgerlijk Wetboek).

Het CBS is voor alle verwerkingen verplicht een verwerkingsgrondslag te hebben. De grondslag van het CBS is afhankelijk van het feit of een verwerking plaatsvindt ten behoeve van een statistisch proces (onder de Wet CBS) of ten behoeve van de bedrijfsvoering.

Ten behoeve van statistische processen

De grondslag voor het CBS voor alle verwerkingen ten behoeve van statistische processen, is grondslag e: taak van algemeen belang of openbaar gezag. Deze grondslag is bedoeld voor (overheids)organisaties die gegevens moeten verwerken om een publieke taak uit te oefenen voor het algemeen belang of openbaar gezag. Een (overheids)organisatie moet bij wet aangewezen zijn om de taak uit te oefenen. Voor het CBS is deze wettelijke taak vastgelegd in de Wet CBS.

Ten behoeve van bedrijfsprocessen

De grondslag voor alle overige (bedrijfs)processen die niet gerelateerd zijn aan statistisch onderzoek onder de Wet CBS kan variëren, afhankelijk van het doel van de verwerking. Gegevens over salaris, onkostenvergoedingen en de afgedragen loonbelasting/premie volksverzekeringen zijn bijvoorbeeld nodig voor de uitvoering van de arbeidsovereenkomst, grondslag b 'Uitvoeren van een overeenkomst'. WOO verzoeken of de uitwisseling van loongegevens met de Belastingdienst vallen onder grondslag c 'Wettelijke verplichting' en op basis van grondslag f 'Gerechtvaardigd belang' kan de werkgever bijvoorbeeld vanwege goed werkgeverschap gegevens verwerken over werkdruk of tevredenheid van werknemers.

Ten behoeve van bedrijfsprocessen kan door het CBS nooit een beroep gedaan worden op grondslag e 'Taak van algemeen belang of openbaar gezag'. Personeelsgegevens die het CBS zelf verzamelt en gegevens die verwerkt worden ten behoeve van de Wet CBS mogen derhalve nooit met elkaar in aanraking komen. De privacycoördinatoren en de Chief Privacy Officer kunnen adviseren over de grondslag bij nieuwe verwerkingen met personeelsgegevens.

3.2 Beginsel b) van de AVG: doelbinding

Organisaties mogen persoonsgegevens alleen verzamelen met een gerechtvaardigd doel. Dat doel moet specifiek zijn en vooraf uitdrukkelijk zijn omschreven. De algemene doelbinding is beschreven in artikel 3 van de Wet CBS. Het CBS heeft tot taak het van overheidswege verrichten van statistisch onderzoek (en het bevorderen van een statistische informatievoorziening) ten behoeve van praktijk, beleid en wetenschap en het openbaar maken van de op grond van zodanig onderzoek samengestelde statistieken. De Wet CBS stelt dat de gegevens die het CBS ontvangt ten behoeve van de wettelijke taak van het CBS uitsluitend gebruikt mogen worden voor statistische doeleinden (artikel 37 Wet CBS). Ook het verstrekken van gegevens die het CBS verwerkt mag alleen ten behoeve van statistische doeleinden (zie artikel 39 tot en met 41 Wet CBS).

Het CBS ontvangt van andere (overheids)organisaties vaak gegevens die onder een andere grondslag met een ander doel zijn verzameld. Het CBS mag deze gegevens opvragen voor statistische doeleinden (artikel 33 Wet CBS) ook al zijn de gegevens voor andere doeleinden verzameld. De AVG biedt voor statistisch onderzoek hiervoor een mogelijkheid (artikel 5 lid 1 sub b en artikel 89 van de AVG en overweging 50 van de AVG).

De doelbinding voor bedrijfsprocessen moet per verwerking apart bepaald worden en is nooit verenigbaar met de doelbinding vanuit de Wet CBS.

3.3 Beginsel c tot en met f van de AVG

Naast de grondslag en de doelbinding zoals hierboven beschreven kent de AVG nog 4 beginselen:

c) minimale gegevensverwerking: dataminimalisatie. Wat is nodig voor een bepaald doel, kan het met minder of met minder specifieke gegevens? Bij het CBS is daarom het schrijven van een onderzoeksvoorstel een belangrijke stap;

d) juistheid: het wissen of rectificeren van onjuiste of onvolledige gegevens. Dit is niet van toepassing op de verwerking van gegevens in de statistische processen van het CBS (bijvoorbeeld statistische correcties) aangezien statistieken geen directe impact op betrokkenen hebben, m.u.v. steekproeven. Dit is wel van toepassing op bedrijfsprocessen die niet vallen onder de Wet CBS;

e) opslagbeperking: gegevens vernietigen zodra ze niet meer nodig zijn. Het CBS kent bewaar- en vernietigingstermijnen die vastgesteld zijn in de Selectielijst[1] van het CBS in het kader van de archiefwet. Het gaat dan zowel om bewaartermijnen van gegevens ten behoeve van bedrijfsprocessen (zoals sollicitatiebrieven en beoordelingsgesprekken) als om gegevens die verwerkt zijn ten behoeve van de Wet CBS, oftewel ten behoeve van statistische processen. Voor statistische gegevens maakt het CBS maakt hierbij onderscheid tussen drie soorten gegevens:
   - gegevens in de **inputbase** (ruwe gegevens): bewaartermijn van maximaal 2,5 jaar (of periodiciteit plus 1 jaar na afloop van het verslagjaar waarop de gegevens betrekking hebben);
   - gegevens in de **microbase**: langdurige opslag. Deze bestanden blijven langdurig nodig voor het vervaardigen van statistiek en worden vaak ook via Remote Access aan externe onderzoekers ter beschikking gesteld voor statistisch en wetenschappelijk onderzoek. Elke drie jaar moet (voor bestanden die persoonsgegevens bevatten in de microbase) gecheckt worden of langdurige opslag nog steeds geldt;
   - **tussenbestanden:** alle overige bestanden die ontstaan tijdens het statistiekproces worden zo snel mogelijk na afloop van het proces vernietigd (maar uiterlijk na 2,5 jaar);

f) integriteit en vertrouwelijkheid: passende beveiligingsmaatregelen nemen voor bescherming tegen onder meer ongeoorloofde of onrechtmatige verwerking en tegen onopzettelijk verlies, vernietiging of beschadiging. De maatregelen voor het borgen van de integriteit en vertrouwelijkheid vormen ook de basis voor het informatiebeveiligingsbeleid van het CBS.

Het CBS is verantwoordelijk voor de naleving van de beginselen van de AVG en kan dat ook aantonen. Deze verantwoordingsplicht geldt zowel naar betrokkenen toe (dat gebeurt o.a. via onze website) als naar interne en externe auditors en toezichthouders toe (documenteren en rapporteren).

3.4 Privacy by design en privacy by default

Om aan de beginselen van de AVG tegemoet te komen stelt de AVG een verwerkingsverantwoordelijke verplicht tot gegevensbescherming door ontwerp (artikel 25 lid 1 AVG) en gegevensbescherming door standaardinstellingen (artikel 25 lid 2 AVG). Deze verplichtingen zijn beter bekend onder de Engelse begrippen 'Privacy by design' en 'Privacy by default'. De European Data Protection Board (EDPB) heeft hiervoor richtsnoeren[2] opgesteld, zie Richtsnoeren over gegevensbescherming door ontwerp en door standaardinstellingen. Hieronder staat een korte toelichting van de begrippen en in de volgende paragraaf staan de generieke uitgangspunten van het Privacybeleid van het CBS die hier invulling aan geven. In hoofdstuk 4 wordt er uitgebreider stilgestaan bij de Privacy by Design strategieën voor het CBS.

[1] Selectielijst CBS: https://www.nationaalarchief.nl/archiveren/kennisbank/selectielijst-van-het-centraal-bureau-voor-de-statistiek-cbs-vanaf-2004-en-de

[2] Richtsnoeren zijn niet-bindende besluiten die de grote lijnen op een bepaald beleidsterrein in de Europese Unie uitzetten. Richtsnoeren zijn zelf weliswaar niet bindend, maar zijn vaak het kader waarin vervolgens wel bindende besluiten worden genomen.

Privacy by design
Privacy by design is de verplichting van het CBS om passende technische en organisatorische maatregelen en noodzakelijke waarborgen in de verwerking in te bouwen. Een technische of organisatorische maatregel of waarborg kan van alles zijn, van de toepassing van geavanceerde technische oplossingen tot de basisopleiding van personeel. Het idee is om al in een vroeg stadium zowel technisch als organisatorisch een zorgvuldige omgang met persoonsgegevens af te dwingen. Het houdt in dat er al bij de ontwikkeling van producten en diensten aandacht moet zijn voor privacy. Doeltreffendheid staat hierbij centraal en is contextafhankelijk. Artikel 25 van de AVG geeft daarom geen lijst met verplichte specifieke technische en organisatorische maatregelen. Wel geeft de AVG een aantal elementen waar rekening mee moet worden gehouden bij het vaststellen van de maatregelen:

- stand van de techniek. Door technologische ontwikkelingen kan een technische maatregel die in het verleden een adequaat niveau van bescherming bood, niet langer toereikend zijn. Dit kan leiden tot niet-naleving van artikel 25 van de AVG. Naast de technische maatregelen moet tegelijkertijd aandacht geschonken worden aan de organisatorische maatregelen die daarmee gepaard gaan. Een gebrek aan passende organisatorische maatregelen kan de doeltreffendheid van een (nieuwe) technologie verminderen of zelfs volledig ondermijnen. Denk bijvoorbeeld aan het rechtenbeheer op mappen. Wanneer de rechten niet adequaat worden bijgehouden (organisatorisch) dan ondermijnt dit de technische doeltreffendheid en kan dit schijnveiligheid creëren. Risico's zijn hiermee niet inzichtelijk;
- de uitvoeringskosten (proportionaliteit). Het CBS hoeft geen onevenredige hoeveelheid middelen te besteden wanneer er andere maatregelen bestaan die minder middelen in beslag nemen, maar ook doeltreffend zijn. De kosten van de uitvoering vormen echter slechts één van de factoren en zijn geen reden op zichzelf om deze vorm van gegevensbescherming niet uit te voeren;
- de aard, de omvang, de context en het doel van de verwerking. De aard kan worden opgevat als de inherente kenmerken van de verwerking, bijvoorbeeld bijzondere categorieën persoonsgegevens, automatische besluitvorming of belemmeringen voor de betrokkene bij het uitoefenen van de rechten. De omvang verwijst naar de grootte en het bereik van de verwerking. De context houdt verband met de omstandigheden van de verwerking, die een invloed kunnen uitoefenen op de verwachtingen van de betrokkene, terwijl het doel betrekking heeft op de doelstellingen van de verwerking;
- de risicobeoordeling. Het CBS is verplicht een risicobeoordeling uit te voeren (artikel 24, 25, 32 en 35 van de AVG) teneinde passende technische en organisatorische maatregelen te identificeren om individuen en hun persoonsgegevens te beschermen en aan de voorschriften van de AVG te voldoen. De risicobeoordeling wordt een Data Protection Impact Assessment (DPIA) genoemd en komt uitgebreid aan bod in hoofdstuk 5.

Privacy by default
Privacy by default is onderdeel van privacy by design. Privacy by default vereist dat de standaardinstellingen altijd zo privacyvriendelijk mogelijk zijn. Dit wordt specifiek toegepast op de uitvoering van het beginsel van minimale gegevensverwerking. Dit houdt in dat het CBS standaard niet méér gegevens verzamelt dan nodig is, de verzamelde gegevens niet in grotere mate verwerkt dan nodig is voor het beoogde doel, de gegevens niet langer bewaard worden dan nodig is en de toegang tot de gegevens beperkt is tot wie dat nodig heeft. Persoonsgegevens mogen niet zonder menselijke tussenkomst voor een onbeperkt aantal natuurlijke personen toegankelijk worden gemaakt (zie artikel 25 lid 2 AVG).

Privacy by design en privacy by default worden vanaf nu als één noemer Privacy by Design (PbD) aangeduid. In de volgende paragraaf staan eerst een aantal generieke privacymaatregelen beschreven die kenmerkend zijn voor heel CBS. In hoofdstuk 4 wordt vervolgens het PbD beleid nader toegelicht dat het uitgangspunt vormt voor de scala aan maatregelen die het CBS toepast bij allerlei verwerkingen nu en in de toekomst.

3.5 Generieke uitgangspunten CBS Privacybeleid

Een 'passende privacymaatregel' is de uitkomst van een afweging tussen het privacyrisico en de 'kosten' van de maatregel.

De AVG laat ruimte aan de verwerkingsverantwoordelijke voor beslissingen over welke maatregelen er genomen moeten worden. Dat is bewust gedaan omdat technologische en organisatorische werkwijzen steeds veranderen. Daarbovenop varieert het per organisatie welke maatregelen het meest geschikt zijn, want niet iedere organisatie is hetzelfde en werkt met dezelfde gegevens voor hetzelfde doel. Het CBS heeft voor de gehele organisatie generieke maatregelen genomen die alle statistische gegevens beschermen waar het CBS mee werkt. Deze uitgangspunten zijn ook toegelicht op de CBS-website en in de CBS Data Protection Impact Assessement (DPIA). Hieronder een beknopt overzicht van de generieke maatregelen voor statistische processen.

Het CBS verwerkt gegevens uitsluitend voor statistische en wetenschappelijke doeleinden
De toegang tot de gegevens die het CBS ontvangt vanuit de Wet CBS is alleen mogelijk voor degenen die belast zijn met de uitvoering van de wettelijke taak van het CBS en die in dat kader noodzakelijkerwijs toegang moeten hebben tot de betreffende data (doelbinding). Het CBS heeft beleid en procedures geïmplementeerd die waarborgen dat de gegevens uitsluitend voor wetenschappelijke en statistische doeleinden kunnen worden gebruikt. Deze doelbinding komt voort uit onder andere internationale regelgeving (artikel 2 lid 1 onder e van de Verordening (EG) Nr. 223/2009 betreffende de Europese statistiek, beginsel 5 van de Praktijkcode voor Europese Statistieken) als in nationale wetgeving (artikel 37 van de Wet CBS). Gebruik van de gegevens voor fiscale, administratieve, controle en gerechtelijke doeleinden is niet toegestaan (zie de memorie van toelichting[3] bij artikel 37 lid 1 Wet CBS).

Publicaties van het CBS zijn nooit te herleiden naar individuele personen, huishoudens, ondernemingen en instellingen
Zoals eerder beschreven vraagt het CBS alleen gegevens op ten behoeve van statistisch onderzoek en publiceert welke gegevens verwerkt worden en op welke wijze (verantwoording). Publicatie is alleen in geaggregeerde vorm toegestaan. Artikel 37 van de Wet CBS stelt: 'gegevens worden slechts zodanig openbaar gemaakt dat daaraan geen herkenbare gegevens over een afzonderlijk persoon, huishouden, onderneming of instelling kunnen worden ontleend, tenzij, ingeval het gegevens met betrekking tot een onderneming of instelling betreft, er een gegronde reden is om aan te nemen dat bij de betrokken onderneming of instelling geen bedenkingen bestaan tegen de openbaarmaking'. Het uitgangspunt bij statistiek is niet-herleidbaar publiceren. Met publiceren op instellingsniveau wordt dan ook terughoudend omgegaan bij het CBS. De vraag of publicatie op ondernemings- of instellingsniveau mogelijk is, wordt onder meer getoetst aan de Beleidsregel publiceren op instellingsniveau artikel 41 Wet CBS[4] en kan worden voorgelegd aan de ethische commissie van het CBS.

Hoewel de publicaties zelf niet onder de AVG vallen, wordt het proces tot publiceren als een verwerking gezien en valt hiermee onder de AVG. Om te zorgen dat publicaties van het CBS nooit te herleiden zijn naar individuele personen, huishoudens, ondernemingen en instellingen voert het CBS zogeheten outputcontroles uit. Alle output van het CBS wordt vóór publicatie gecontroleerd op onthullingsrisico. Daarbij wordt ook gekeken naar de relaties met eerdere en andere gelijktijdige publicaties van het CBS. Bij mogelijke onthullingsrisico's worden er maatregelen getroffen, zoals het samenvoegen van publicatiecellen (aggregeren) of het verwijderen van celwaarden (onderdrukken). Daartoe is door het CBS in Europees verband software ontwikkeld. Alle output wordt gecontroleerd voordat het daadwerkelijk wordt gepubliceerd. Het gehele proces tot publicatie valt bij het CBS onder het thema van statistische beveiliging.

[3] Tweede Kamer, vergaderjaar 2001–2002, 28 277, nr. 3 (MvT), p. 36.

[4] Beleidsregel van de directeur-generaal van de statistiek van 17 april 2023, nr. CSB-2023-056, met betrekking tot het publiceren op instellingsniveau van statistisch onderzoek op gegevens van het CBS op grond van artikel 41 Wet CBS: Beleidsregel publiceren op instellingsniveau artikel 41 Wet CBS

Het CBS pseudonimiseert de gegevens zo snel mogelijk
De AVG noemt pseudonimiseren als expliciet voorbeeld van een technische en organisatorische maatregel (artikel 25 AVG) om gegevens te beschermen. Bij het CBS worden persoonsgegevens zo snel mogelijk gepseudonimiseerd. Dit houdt in dat direct identificerende gegevens zoals naam, adres, Burgerservicenummer (BSN) en andere direct identificerende kenmerken worden verwijderd en vervangen door een pseudoniem, een Record Identificatienummer (RIN). In dit proces worden ook minder identificerende kenmerken geaggregeerd, zoals geboortedatum naar maand en jaar. De analyses worden vervolgens uitgevoerd op de gepseudonimiseerde bestanden.

Voor bedrijfsgegevens geldt dat de gegevens gepseudonimiseerd worden zodra dit mogelijk is. Voor bedrijven geldt het Bedrijfsidentificatie-nummer (BE_ID) in plaats van het RIN. In tegenstelling tot persoonsstatistieken waarbij het individu niet relevant is voor het statistisch proces, is het voor de bedrijfsstatistieken vaak wel noodzakelijk te weten om welk individueel bedrijf het gaat, bijvoorbeeld bij kwaliteitscontroles. Dit geldt alleen voor de grote bedrijven. Voor bedrijfsgegevens geldt daarom dat er een duidelijk proces met motivatie moet zijn voor de processen waarvoor pseudonimisering of anonimisering pas ná de analysefase kan plaatsvinden. Ook blijft het CBS continu aandacht besteden aan verbetertrajecten om pseudonimisering gedeeltelijk automatisch te kunnen toepassen op delen van populaties zoals ZZP'ers en kleine ondernemingen.

Werknemers van het CBS hebben als ambtenaar een eed of belofte afgelegd en zijn verplicht tot geheimhouding conform artikel 5 en 9 van de Ambtenarenwet 2017.

Toegang CBS-data voor externe onderzoekers
Het CBS biedt externe onderzoekers van gecertificeerde instellingen de mogelijkheid onafhankelijk onderzoek te doen op CBS-data via remote access (onderzoek op afstand). Het CBS blijft hiervoor verwerkingsverantwoordelijk en heeft in 2021 de 'Beleidsregel toegang instellingen tot microdata CBS' vastgesteld[5] om duidelijkheid te scheppen over de voorwaarden die het CBS stelt ten aanzien van extern onderzoek op CBS-data. Onderzoekers van externe instellingen dienen te tekenen voor geheimhouding in een overeenkomst en geheimhoudingsverklaring. Ook moeten externe onderzoekers zich aan het CBS-beleid voor Remote Access[6] houden.

Interne en externe toetsing
Het CBS kent (zoals beschreven in paragraaf 2.3. Privacygovernance) een FG en een interne Auditdienst als interne toezichthouders van het CBS op het gebied van privacy, informatiebeveiliging en kwaliteit. Het CBS laat zich jaarlijks extern toetsen op privacybescherming (Privacy Control Framework van NOREA, informatiebeveiliging (ISO 27001) en kwaliteit (ISO 9001). De certificaten worden op de website van CBS gezet (verantwoording).

Comply or explain
Bovenstaande uitgangspunten gelden voor heel CBS als de standaard. Daarnaast heeft het CBS vele maatregelen en voorzieningen getroffen om gegevensverwerkingen zo veilig mogelijk in te richten. Van beveiligde uploadportals voor bronhouders tot en met verschillende niveaus van werkomgevingen, afhankelijk van de gegevens waarmee wordt gewerkt. Ook biedt het CBS standaard programma's en middelen aan zijn personeel om veilig te kunnen werken. Software, programma's en diensten die niet door het CBS worden aangeboden mogen dan ook niet gebruikt worden voor verwerkingen, tenzij dit door de security afdeling is goedgekeurd en alle privacyrisisco's zijn geadresseerd. Ook zijn er gedragsregels opgesteld waar elke medewerker zich aan moet houden.

Afwijken van de standaard mag alleen gebeuren als daar een geldige reden voor is en het anders niet mogelijk is om de wettelijke taak van het CBS uit te oefenen (comply or explain). In dat geval vindt er een belangenafweging plaats: doel en noodzaak versus de impact en risico's

[5] https://wetten.overheid.nl/BWBR0045454/2021-08-01
[6] https://www.cbs.nl/nl-nl/onze-diensten/maatwerk-en-microdata/microdata-zelf-onderzoek-doen

voor betrokkenen. Deze belangenafweging en het uiteindelijke besluit worden door de eerste lijn gemaakt en vastgesteld.

Om te voldoen aan de beginselen van de AVG is het, naast de algemene maatregelen, ook nodig om per individuele verwerking aandacht te besteden aan de beginselen van de AVG. Vooral wanneer het nieuwe bronnen, methoden en technieken, nieuwe revisies en nieuwe technische toepassingen en diensten betreft. Ook kunnen externe factoren nieuwe risico's opwerpen of kunnen er door de stand van de techniek nieuwe risico's of juist beveiligingsmogelijkheden ontstaan. Bij het CBS is privacybescherming nauw verweven met informatiebeveiliging. Dit wordt verder geconcretiseerd door middel van de Privacy by Design strategieën in Hoofdstuk 4 en het risicomanagement in hoofdstuk 5.

4. Privacy by Design strategieën

Het CBS is een dataorganisatie. De wettelijke taak van het CBS is het vervaardigen van statistisch onderzoek en vanuit deze taak ontvangt het CBS heel veel overheidsregistraties en bedrijfsregistraties met gegevens over alle personen in Nederland. Om die reden hebben alle verwerkingen in principe een hoog risico voor betrokkenen vanwege de hoeveelheid gegevens die van alle burgers in Nederland samenkomen op het CBS.

Aangezien het CBS veel verwerkingen kent vanuit dezelfde wettelijke taak (het doen van statistisch onderzoek) kan PbD generiek ingezet worden zoals toegelicht in hoofdstuk 3. Maar daarmee is het CBS nog niet klaar. PbD is een continu proces, mede doordat technologische ontwikkelingen snel gaan. De meest effectieve wijze om PbD gestructureerd toe te passen is door PbD proactief mee te nemen bij nieuwe initiatieven zoals bij het inkopen van nieuwe producten, programma's en toepassingen, in de voorbereidende fase van nieuwe statistieken, maar ook aan de start van omvangrijke revisies van bestaande statistieken. In al deze situaties zijn dit logische momenten om PbD in een vroeg stadium mee te nemen. Het proactief meenemen van PbD is effectiever dan wanneer achteraf blijkt door middel van risicoanalyses, dat er aanvullende maatregelen genomen moeten worden. Daarnaast is het ook van belang dat bestaande verwerkingen regelmatig geëvalueerd worden vanuit de PbD strategieën. Op deze wijze blijft het CBS continu verbeteren.

4.1 De Acht Privacy-ontwerpstrategieën

Om PbD te concretiseren heeft Dr. J.H. Hoepman acht Privacy-ontwerpstrategieën[7] ontwikkeld die veelal gebruikt worden als concreet sturingsinstrument. Ook het CBS gebruikt dit als basis voor het PbD beleid. Deze Privacy-ontwerpstrategieën zijn onderverdeeld in twee groepen: datageoriënteerde strategieën en procesgeoriënteerde strategieën, zie figuur 1 op de volgende pagina. Deze strategieën zijn vertaald naar de CBS situatie en vormt het uitgangspunt van het privacy-by-design-beleid van het CBS.

Hieronder wordt per strategie een toelichting gegeven met enkele concrete voorbeeldvragen voor het CBS. Het is geen uitputtende lijst. Het idee van PbD is juist dat men kritische vragen blijft stellen. De stand van de techniek, maatschappelijke ontwikkelingen en wettelijke veranderingen zorgen immers voor veranderende omstandigheden.

[7] Hoepman, J.H. (2020). Privacyontwerpstrategieën, *Het Blauwe Boekje*. https://www.cs.ru.nl/~jhh/publications/pds-boekje.pdf

Figuur 1. De acht Privacy-ontwerpstrategieën

4.2 Datageoriënteerde strategieën

1. Minimaliseer

Doelbinding: het CBS heeft een generieke doelbinding vanuit de Wet CBS. Dat betekent echter niet dat er onbeperkt gegevens verzameld mogen worden. Per verwerking moet er een concreet doel zijn. Je mag dus niet méér gegevens opvragen en verwerken dan je nodig hebt voor een specifieke statistiek waarvoor je de gegevens nodig hebt. Een medewerker van het CBS mag ook geen toegang hebben tot gegevens die bij het CBS aanwezig zijn maar die de medewerker niet nodig heeft voor zijn of haar werk.

Bewaartermijnen: het CBS heeft standaard bewaartermijnen voor alle gegevens waarmee gewerkt wordt, zie ook de Selectielijst van het CBS. Zie ook de toelichting bij paragraaf 3.2.

Proportionaliteit en subsidiariteit: proportionaliteit betekent dat het doel van de verwerking van de persoonsgegevens in verhouding moet staan tot de inbreuk op de privacy van de betrokkene. Is het bijvoorbeeld nodig om sollicitatiegegevens langer dan vier weken te bewaren na afloop van een sollicitatieprocedure?

Subsidiariteit betekent dat als het doel op een andere manier bereikt kan worden, die minder ingrijpend is voor de betrokkenen, dat je dat moet doen. Hierbij is de doelbinding erg belangrijk. Stel er wordt een statistiek gemaakt over drukte in het openbaar vervoer. Is het dan nodig om van elke passagier het hele jaar door het exacte tijdstip van in-en uitchecken te verzamelen of kan worden volstaan met een tijdsframe van een uur.

Relevante vragen zijn:

- Over hoeveel personen worden gegevens verzameld? Kan het wellicht ook met een steekproef?
- Hoeveel informatie wordt er verzameld? Kan het doel ook bereikt worden met minder gegevens of minder specifieke gegevens?
- Kan het detailniveau van de informatie wellicht omlaag?
- Over welke periode worden de gegevens verzameld?

2. Scheid

Compartimenteer. Door gegevens gescheiden op te slaan en te verwerken, wordt het risico op datalekken verkleind. Enerzijds zorgt het ervoor dat personen niet bij gegevens kunnen die ze niet nodig hebben voor hun werk. Anderzijds loopt de organisatie minder risico bij bijvoorbeeld een datalek. Scheiding van gegevens kan op verschillende manieren:

- isoleer door middel van logisch gescheiden databases of systemen. Denk hierbij aan de rechtenstructuur en toegangsbeheer, bijvoorbeeld de autorisaties die het CBS toekent aan personen tot specifieke opslagmiddelen waar gegevens in staan. Het CBS kent verschillende werkomgevingen (productieomgeving, testomgeving, secure (SEC) omgevingen, ontwikkelomgeving(ONT)). Afhankelijk van het werk heeft een medewerker toegang tot bepaalde werkomgevingen en gegevens van de éne werkomgeving kan niet zonder meer uitgewisseld worden met gegevens in een andere werkomgeving;
- *logische scheiding van soorten gegevens. Denk bijvoorbeeld aan het scheiden van* identificerende en gepseudonimiseerde gegevens. Wanneer deze soorten gegevens bij elkaar worden opgeslagen zal dit namelijk het effect van pseudonimisering teniet doen. Ook kunnen bijzondere persoonsgegevens apart opgeslagen worden voor extra autorisatie of controle, of kunnen gegevens gescheiden worden die niets met elkaar te maken hebben;
- *project- of processpecifieke encryptie.* Dit zorgt ervoor dat verschillende databases met gegevens niet eenvoudig aan elkaar te koppelen zijn. Momenteel onderzoekt het CBS hoe dit gerealiseerd kan worden, bijvoorbeeld door extra versleuteling per proces (de proces specifieke RIN oftewel, de PRIN). Dat zou inhouden dat als een medewerker aan twee statistieken werkt, dat door aparte versleuteling per statistiek de onderzoeker beide bestanden niet aan elkaar kan relateren, ook al staat het in dezelfde omgeving en heeft de medewerker rechten voor beide onderzoeken.

Distribueer. Gegevens kunnen centraal worden opgeslagen in één grote database of ze kunnen worden gedistribueerd over verschillende (decentrale) fysieke locaties.

Een technisch voorbeeld van distribueren is Secure Multi-Party Computation (MPC), een privacy preserving technique waarmee meerdere partijen gezamenlijk aan een databestand kunnen werken zonder dat ze elkaars data kunnen inzien en zonder dat de data de eigen locatie verlaat. Op deze wijze blijven de bestanden gedistribueerd staan op de eigen locatie maar kan het toch gebruikt worden voor een gezamenlijke statistiek.

3. Abstraheer

Aggregatie. Abstraheren door middel van aggregatie behelst bijvoorbeeld het maken van categorieën zoals leeftijdscategorieën of ingedikte variabelen. Bij het CBS wordt in het pseudonimiseerproces standaard de geboortedatum geaggregeerd naar geboortemaand- en jaar. Daarnaast wordt bij ieder onderzoek de vraag gesteld hoeveel detail daadwerkelijk nodig is voor het doel van de verwerking.

Ruis toevoegen. Bij ruis toevoegen wordt niet de precieze waarde van een gegeven gebruikt maar een benadering van de waarde, of wordt de waarde aangepast met een kleine hoeveelheid ruis. Een voorbeeld zijn locatiegegevens in een grid in plaats van precieze GPS-coördinaten.

4. Verberg

Toegangsbeheer. Toegang tot data dient te worden beperkt en de informatiebeveiliging moet op orde zijn. Bij het CBS gebeurt dat via de dataopslag en autorisaties. Onderzoekers krijgen alleen toegang tot de gegevens die ze nodig hebben voor het werk.

Verbreek link. Identificerende gegevens dienen zo snel mogelijk te worden verwijderd. Bij het CBS gebeurt dat door middel van pseudonimisering zo vroeg mogelijk in het proces. Zie ook de generieke maatregelen bij hoofdstuk 3.

Maak onbegrijpbaar of onherleidbaar. Gegevens moeten waar mogelijk worden geanonimiseerd of gepseudonimiseerd. Bij het CBS moeten veel gegevens gekoppeld worden voor statistische analyses. De gegevens worden daarom zo vroeg mogelijk door het CBS gepseudonimiseerd waarbij de direct identificerende kenmerken worden verwijderd. Alle output wordt voor publicatie streng gecontroleerd op statistische onthulling (geanonimiseerd).

4.3 Procesgeoriënteerde strategieën

Naast de datageoriënteerde strategieën zijn er ook vier procesgeoriënteerde strategieën. Deze strategieën zijn vooral gericht op de beleidskant van PbD en sluiten aan bij belangrijke principes van de AVG zoals transparantie en verantwoording. Het gaat om de volgende vier strategieën.

5. Informeer

Het CBS dient transparant te zijn over welke persoonsgegevens het CBS verwerkt, voor welk doel en op welke wijze. Transparantie geldt ook voor informatie over welke gegevens gedeeld worden met derden. Het CBS borgt dit op de privacypagina[8] van de CBS-website, in de methodebeschrijvingen van elke publicatie en op de Remote Acces pagina van de CBS-website. Een afslag van de Algemene Bronnencatalogus (een overzicht van alle gegevens die het CBS verwerkt) staat gepubliceerd op de website en wordt regelmatig geactualiseerd.

6. Geef controle

Dit principe slaat op de mogelijkheid van het opvragen van de gegevens van betrokkenen die door het CBS worden verwerkt en de mogelijkheid voor correctie of verwijdering. Dit wordt in de AVG ook wel ‘de rechten van betrokkenen’ genoemd (artikel 13-18 en 20-22 van de AVG). Voor het CBS is deze strategie verschillend voor bedrijfsprocessen en voor statistische processen. Voor bedrijfsprocessen (denk aan verwerkingen van gegevens over het eigen personeel) moeten de rechten van betrokkenen nageleefd worden. Voor statistische processen ligt dat wat anders. Zo geldt bijvoorbeeld voor artikel 15, 16 en 18 dat deze buiten toepassing gelaten kunnen worden in geval van statistisch onderzoek (zie artikel 44 UAVG). Bij artikel 20 ligt de uitzondering in de Wet CBS en artikel 22 is niet van toepassing.

7. Leef na

Privacy moet niet alleen technisch maar ook in organisatorische zin beschermd worden. Het moet onderdeel zijn van de bedrijfscultuur en uitgedragen worden vanuit de top van de organisatie. Denk hierbij aan:

- het committeren als organisatie aan het Privacybeleid en middelen beschikbaar stellen hiervoor;
- het implementeren en naleven van het beleid;
- het actualiseren van het beleid en de maatregelen, rekening houdend met veranderende wetgeving, maatschappelijke belangen en de technische stand van zaken. In hoofdstuk 5 ‘risicomanagement en DPIA’s’ wordt hier nader op ingegaan;
- ervoor zorgen dat alles ook aangetoond kan worden (zie punt 8).

Het CBS heeft in 2021 een nieuwe privacygovernance ingericht met een Chief Privacy Officer en Privacycoördinatoren om de organisatie te ondersteunen in het naleven van wet-en regelgeving

[8] https://www.cbs.nl/nl-nl/over-ons/dit-zijn-wij/onze-organisatie/privacy

en te adviseren bij het Privacybeleid. Er is een Privacyagenda gekomen die met regelmaat in het hoogste overlegorgaan van het CBS (het Directieberaad) besproken wordt. Tenslotte is privacybescherming een vast onderdeel van het meerjarenplan en het jaarplan van het CBS.

8. Toon aan

Het CBS dient aan te tonen dat het op een privacyvriendelijke wijze gegevens verwerkt. Het CBS toont dit aan door middel van documentatie over verwerkingen en processen door middel van de procesdocumentatie (met als onderdeel de risicoanalyse, de baselinetoets) en het verwerkingenregister. Daarnaast geldt voor alle maatregelen dat deze passend moeten zijn en er dus rekening gehouden moet worden met de risico's, de stand van de techniek, de uitvoeringskosten en de aard en omvang van de verwerking. Tegelijkertijd staat het belang van de betrokkene centraal. Bij de afweging in welke mate een maatregel of een criterium wordt gehanteerd is het belang van de betrokkene leidend. Het CBS zal, wanneer bepaalde datageoriënteerde strategieën niet mogelijk zijn op dat moment, verantwoorden en documenteren hoe de belangenafweging tot stand is gekomen en welke beslissing (met bijbehorend risico) is genomen. Het CBS ontwikkelt hiervoor een pre-DPIA scan die als aanvullende documentatie komt naast de procesdocumentatie (baselinetoets) en de CBS DPIA.

Daarnaast worden er regelmatig interne en externe audits gehouden. Het CBS heeft sinds 2015 het keurmerk Privacy Audit Proof conform het Privacy Control Framework van NOREA, uitgevoerd door Duijnborgh Audit.

4.4 Gebruik en verantwoordelijkheden PbD

PbD moet proactief meegenomen worden bij nieuwe initiatieven Denk hierbij aan:

- nieuwe onderzoeken;
- nieuwe bronnen, methoden en technieken;
- nieuwe of hernieuwde samenwerkingen;
- revisies en herontwerpen;
- nieuwe producten, diensten en toepassingen.

De proceseigenaar (eerste lijn) is verantwoordelijk voor het meenemen van het PbD principe en kan daarbij advies en ondersteuning vragen aan de PC en CPO. Daarbij is een goede belangenafweging noodzakelijk. Privacybescherming is immers één van de belangen die afgewogen moeten worden bij een beslissing. De proceseigenaar moet de belangenafweging maken en een beslissing nemen of een privacymaatregel passend is.

De beslissingsbevoegdheid ligt daarom altijd bij de eerste lijn. Wanneer een datageoriënteerde strategie (bijvoorbeeld pseudonimiseren) niet mogelijk is voor een bepaalde verwerking, dan moet onderzocht worden of door aanvullende maatregelen het risico toch beperkt kan worden (bijvoorbeeld door strikter toegangsbeheer of kortere bewaartermijnen). Ook moet er extra aandacht geschonken worden aan de proces-georiënteerde strategieën zoals het informeren van de buitenwereld (strategie 5) of de verantwoording binnen de organisatie goed vastleggen (strategie 7 en 8). Restrisico's moeten opgenomen worden in het risicoregister (zie hoofdstuk 5) zodat er regelmatig geëvalueerd wordt of een strategie in een later stadium wel doorgevoerd kan worden (comply or explain). Het uitgangspunt is dat actief voldoen aan het PbD kader in een later stadium minder werk betekent, en meer verantwoorden en regulier evalueren wanneer er sprake is van uitzonderingen of afwijking met extra risico's. Op deze wijze geeft het CBS vorm aan het continu verbeteren op het gebied van privacybescherming.

5. Risicomanagement en DPIA

Risicomanagement is een doorlopend proces en is verplicht vanuit de AVG. Het instrument voor een risicoanalyse is de Data Protection Impact Assessment (DPIA), ook wel een gegevensbeschermingseffectbeoordeling (GEB) genoemd. Een DPIA is een instrument om vooraf de privacyrisico's van een gegevensverwerking in kaart te brengen, zodat de organisatie maatregelen kan nemen om deze risico's te verkleinen. Een DPIA is verplicht wanneer een organisatie van plan is om persoonsgegevens te verwerken en deze verwerking waarschijnlijk een hoog privacyrisico oplevert.

De Nederlandse toezichthouder, de Autoriteit Persoonsgegevens (AP) heeft een lijst[9] opgesteld van soorten verwerkingen waarvoor het uitvoeren van een DPIA verplicht is. Omdat het CBS op grote schaal gegevens verwerkt moet het CBS voor alle statistische processen een DPIA opstellen. Vergelijkbare verwerkingen met vergelijkbare risico's kunnen door middel van één DPIA beoordeeld en gemitigeerd worden. Het CBS heeft daarom een CBS brede DPIA voor alle standaard statistische processen van verwerkingen, de CBS DPIA[10]. Deze is gepubliceerd op de website van het CBS en wordt periodiek herzien. Voor verwerkingen die buiten de standaard statistische processen vallen moeten aanvullende DPIA's opgesteld worden.

Ook al zijn de CBS brede risico's geanalyseerd en zijn er mitigerende maatregelen genomen, door voortschrijdend inzicht kunnen bij bestaande verwerkingen nieuwe risico's ontstaan. Denk aan nieuwe technologische ontwikkelingen, maatschappelijke ontwikkelingen en nieuwe wet- en regelgeving. Ook kunnen maatregelen die tien jaar geleden effectief waren nu of in de toekomst niet meer toereikend zijn. Daarnaast ontstaan er continu nieuwe verwerkingen, door bijvoorbeeld nieuwe bronnen, methoden en technieken, nieuwe samenwerkingen, grote revisies of nieuwe risicovolle onderzoeken. Risicomanagement vraagt daarom continu aandacht.

Verschil risicomanagement informatiebeveiliging en privacybescherming

Het risicomanagement voor privacybescherming zal in grote lijnen vergelijkbaar zijn met een risicoafweging in het kader van informatiebeveiliging. Daarom kan gebruik gemaakt worden van informatie die daaruit naar voren komt. Echter, er zit een wezenlijk verschil tussen het risicomanagement ten aanzien van informatiebeveiliging en van privacybescherming.

Risicomanagement informatiebeveiliging: het proces van het identificeren en beheersen van de risico's waaraan een organisatie is blootgesteld.

Risicomanagement privacybescherming: het proces van het identificeren en beheersen van de risico's van de gegevensverwerkingen voor de rechten en vrijheden van de betrokkenen.

Informatiebeveiliging is een belangrijke voorwaarde voor een adequate privacybescherming, maar het is slechts een onderdeel ervan. Zo zijn er situaties denkbaar waarin de informatie adequaat beschermd wordt, maar bijvoorbeeld de resultaten van een statistiek of methodiek een impact hebben op een betrokkene, of een groep betrokkenen. Hoewel het CBS geen invloed heeft op hoe andere organisaties de gepubliceerde tabellen van het CBS gebruiken, is het vanuit privacybescherming wel relevant om vooraf goed de risico's van een onderzoek voor betrokkenen te identificeren.

---

[9] https://www.autoriteitpersoonsgegevens.nl/documenten/besluit-lijst-verplichte-dpia

[10] https://www.cbs.nl/-/media/cbs/over-ons/organisatie/standaardcbspia-2021-v20.pdf

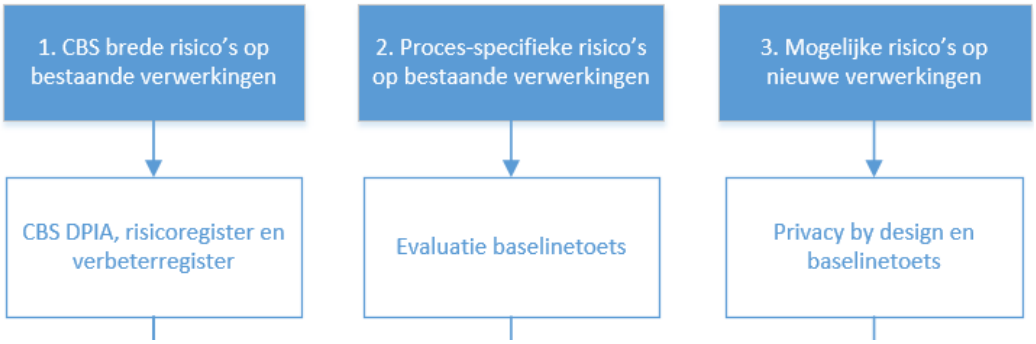
Daarnaast is dit ook relevant wanneer het CBS vanuit bedrijfsvoering gegevens van het eigen personeel verwerkt. Vanuit informatiebeveiliging kan dit goed uitvoerbaar zijn, maar het verwerken van gegevens van het eigen personeel valt niet onder de Wet CBS. De betrokkenen zijn in dit geval het eigen personeel. Het maakt hierbij niet uit of het gaat om het meten van de werkdruk, de medewerkerstevredenheid of om vanuit goed werkgeverschap diversiteit en gelijkheid te willen bevorderen. In alle gevallen moet onderzocht worden of deze verwerkingen risico's voor de betrokkenen kunnen opleveren. Er is immers sprake van een werkgever – werknemer relatie. Ook is de betrokkene in deze gevallen gerechtigd controle uit te oefenen op de verwerking van de eigen gegevens (rechten van betrokkenen zoals beschreven in artikel 13-18 en 20-22, van de AVG).

Het risicomanagement bestaat uit de volgende drie stappen die in de volgende paragrafen worden toegelicht:

1. risico's identificeren;
2. risico's inschatten en analyseren;
3. risico's beoordelen, mitigeren en evalueren.

5.1 Risico identificeren

Het risicomanagement voor privacybescherming bestaat uit een aantal stappen. Als eerste stap moeten de risico's geïdentificeerd worden. De identificatie van de risico's kan op vele manieren, proactief of per toeval, bijvoorbeeld naar aanleiding van een datalek. Om structuur aan te brengen in het risicomanagement worden drie categorieën van risico identificatie onderscheiden:



1. CBS brede risico's op bestaande verwerkingen

Zoals eerder beschreven heeft het CBS voor alle bestaande standaard verwerkingen centraal mitigerende maatregelen, zoals het pseudonimiseerproces, rechtenbeheer en toegang, en outputcontroles. Deze staan beschreven in de CBS DPIA. Dit is een dynamisch document. Door technologische en maatschappelijke ontwikkelingen en door nieuwe standaard processen moeten deze CBS brede risico's regulier opnieuw geïdentificeerd, geanalyseerd en gemitigeerd worden. De identificatie van deze CBS brede risico's kan op allerlei wijzen gebeuren, via FG adviezen, datalekken of door proactieve inventarisaties door experts en stakeholders. Proactieve inventarisaties worden op vaste momenten uitgevoerd (bijvoorbeeld voorafgaand aan de reguliere update van de CBS DPIA). Overige risico's kunnen op elk moment geïdentificeerd worden. Nieuwe risico's worden geadresseerd en bijgehouden in het risicoregister/verbeterregister.

2. Proces-specifieke risico's op bestaande verwerkingen

Risicomanagement per proces is al geborgd in de Baselinetoets privacybescherming en informatiebeveiliging (onderdeel van de procesdocumentatie). Vooraf aan iedere verwerking wordt er een risicoanalyse uitgevoerd op de privacy-en beveiligingsaspecten. Dit gebeurt aan de hand van een Baseline(toets). Doel van deze toets is om vast te stellen of voor een onderhavig proces voldoende maatregelen genomen zijn om risico's, op het gebied van privacybescherming en informatiebeveiliging, tot een aanvaardbaar niveau te reduceren. Met andere woorden, of

het proces voldoet aan de eisen van privacy- en beveiligingsnormen. De Baselinetoets geldt voor zowel statistische verwerkingen als voor verwerkingen voor de bedrijfsvoering.

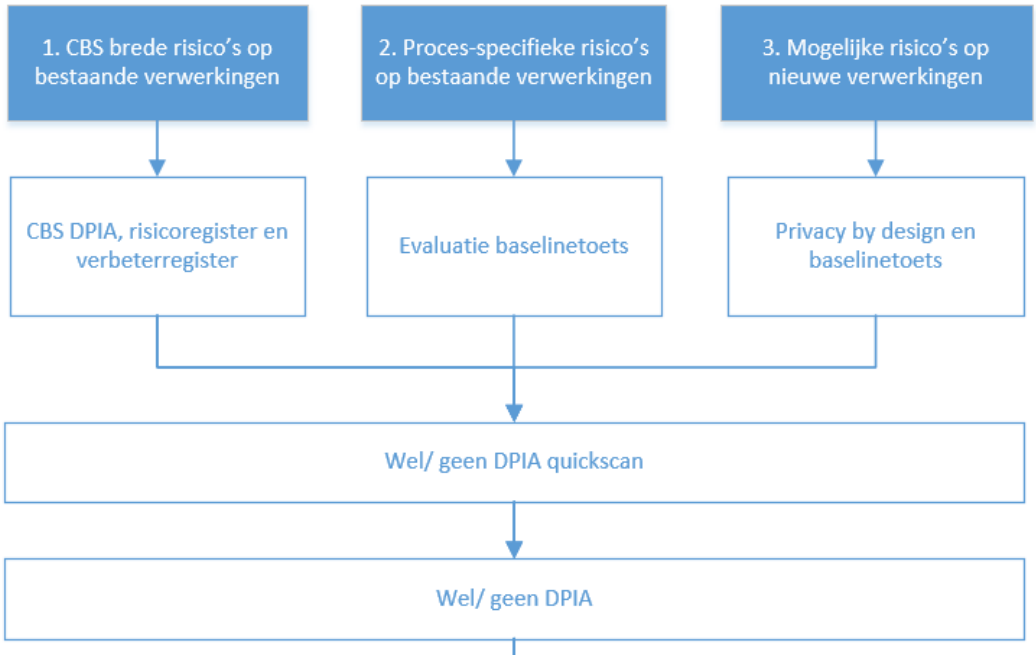
Het CBS beleid is dat deze Baselinetoetsen jaarlijks worden geëvalueerd door de proceseigenaar. Op deze wijze is geborgd dat nieuwe risico's die ontstaan op bestaande processen tijdig geïdentificeerd worden. Dit proces wordt op steekproefbasis getoetst door de interne auditdienst en jaarlijks getoetst in de externe privacyaudit.

3. Mogelijke risico's op nieuwe verwerkingen

Onder nieuwe verwerkingen verstaan we: nieuwe bronnen, methoden en technieken, nieuwe producten en diensten, grote revisies van statistieken en verbetertrajecten, nieuwe samenwerkingen en nieuwe onderzoeken met een mogelijk hoog risico voor betrokkenen. Voor al deze verwerkingen geldt dat er mogelijk aanvullende risico's zijn die niet geadresseerd zijn in de CBS standaard DPIA. Het Privacy by Design model met strategieën is bedoeld om in een vroeg stadium bij nieuwe verwerkingen mogelijke risico's te identificeren en proactief te mitigeren.

5.2 Risico's inschatten en analyseren

Na identificatie worden de risico's ingeschat en geanalyseerd. Zoals eerder gezegd is de DPIA het instrument daarvoor. Echter, niet voor alle risico's is een DPIA noodzakelijk, bijvoorbeeld wanneer de risico's niet groot blijken en er al maatregelen bedacht zijn om de nieuwe risico's te mitigeren. Om in te schatten of een DPIA noodzakelijk is, wordt er eerst een DPIA quickscan uitgevoerd. Aan de hand van de DPIA quickscan wordt beoordeeld of een uitgebreide DPIA noodzakelijk is.



5.3 Risico's beoordelen, mitigeren en evalueren.

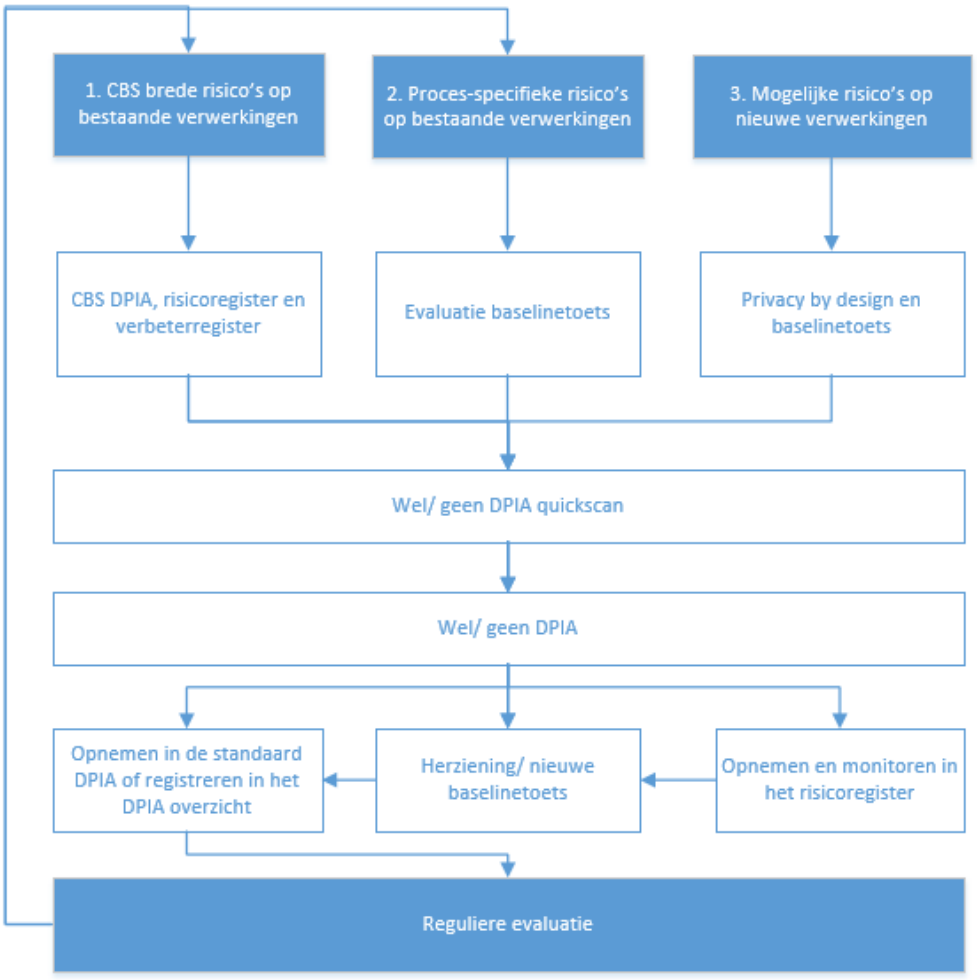
Na de quickscan zijn er drie opvolgingsacties:

1. De risico's zijn al gemitigeerd met bestaande maatregelen. In dat geval wordt de baselinetoets indien nodig herzien en opgeslagen bij de procesdocumentatie.
2. De risico's kunnen met eenvoudige nieuwe maatregelen die al bedacht zijn gemitigeerd worden. In dat geval worden de risico's opgeslagen in het risicoregister/verbeterregister en wordt daarin ook de voortgang en verantwoording gedocumenteerd. Wanneer de maatregelen uitgevoerd zijn wordt de baselinetoets herzien indien nodig en wordt de quickscan gedocumenteerd bij de procesdocumentatie.

3. Er is een aanvullende DPIA nodig. In dat geval wordt er een DPIA geschreven en de mitigerende maatregelen uit deze DPIA worden in het risicoregister/verbeterregister opgeslagen en de voortgang en verantwoording gedocumenteerd. Wanneer de maatregelen uitgevoerd zijn wordt de baselinetoets herzien indien nodig en wordt de DPIA gedocumenteerd bij de procesdocumentatie.

Het risicoregister/verbeterregister en de DPIA's worden verder centraal opgeslagen. De Baselinetoets en de DPIA worden lokaal bij de procesdocumentatie opgeslagen.

Risicomanagement is een dynamisch proces. Het is daarom belangrijk om met regelmaat te onderzoeken of er mogelijke nieuwe risico's ontstaan ten aanzien van bestaande verwerkingen. Om die reden wordt de standaard CBS DPIA regulier herzien en wordt de Baselinetoets jaarlijks geëvalueerd en herzien indien nodig. Voor nieuwe verwerkingen waarvoor een DPIA is opgesteld wordt geadviseerd om de DPIA in verschillende fases van de uitvoering te evalueren. Gedurende het proces van een nieuwe verwerking kunnen immers aanvullende risico's geïdentificeerd worden. Ook wordt geadviseerd na afronding van de DPIA alvast een evaluatie in te plannen om te analyseren of de DPIA alle risico's heeft geadresseerd.



Bijlage 1. Relevante wet- en regelgeving

Wet- en regelgeving in het kader van privacy vinden we terug in alle lagen van de wet. Zowel op Europees en nationaal niveau als in specifieke wetgeving voor een bepaald thema. Bij het opstellen van dit Privacybeleid is rekening gehouden met de AVG, de UAVG en de Wet CBS.

De Algemene Verordening Gegevensbescherming (AVG) Verordening (EU) 2016/679 van het Europees Parlement en de Raad
Sinds 25 mei 2018 is de Algemene Verordening Gegevensbescherming rechtstreeks van toepassing in alle lidstaten van de Europese Unie. Het doel van de AVG is om twee belangen te waarborgen: de bescherming van natuurlijke personen in verband met de verwerking van hun gegevens en het vrije verkeer van persoonsgegevens binnen de Europese Unie. De AVG zorgt er voor dat de privacyrechten van burgers worden versterkt en uitgebreid, dat er meer verantwoordelijkheden zijn voor organisaties (denk aan een documentatie- en een verantwoordingsplicht) en dat de Autoriteit Persoonsgegevens meer bevoegdheden heeft (boetebevoegdheid).
Relevante artikelen AVG:
- Artikel 4: definities;
- Artikel 5: beginselen inzake de verwerking van persoonsgegevens;
- Artikel 6: rechtmatigheid van de verwerking;
- artikel 13-18 en 20-22: rechten van de betrokkene;
- Artikel 25 en Grond 78: privacy by default en by design;
- Artikel 35: DPIA (Gegevensbeschermingseffectbeoordeling);
- Artikel 89: waarborgen en afwijkingen in verband met o.a. wetenschappelijk onderzoek of statistische doeleinden.

Uitvoeringswet Algemene verordening gegevensbescherming (UAVG)
De AVG is rechtstreeks van toepassing in Nederland. Daar waar de AVG ruimte laat voor nationale keuzes bij de uitvoering van de AVG, zijn deze ingevuld in de Uitvoeringswet AVG (UAVG). Daarnaast regelt deze wet de instelling en inrichting van de Autoriteit Persoonsgegevens (AP) als nationale toezichthouder.

Wet op het Centraal Bureau voor de Statistiek
De wettelijke grondslag voor CBS is nationaal geborgd in de Wet op het Centraal Bureau voor de Statistiek (Wet CBS) en internationaal in de Verordening betreffende de Europese statistiek (EG nr. 223/2009) en de daaraan gelieerde Praktijkcode voor Europese statistieken. Beide wettelijke kaders sluiten nauw aan op de AVG. Waar de AVG zich echter beperkt tot persoonsgegevens, zijn de Wet CBS en de hiervoor genoemde Verordening tevens van toepassing op gegevens van ondernemingen en instellingen. Het Privacybeleid van het CBS is dus van toepassing op álle gegevens die het CBS ontvangt. De volgende specifieke artikelen uit de Wet CBS zijn relevant voor het Privacybeleid van het CBS:
- Artikel 3, 4 en 5: wettelijke taak en tevens grondslag voor rechtmatige verwerking en de doelbinding;
- Artikel 33: gegevensverwerving;
- Artikel 34: gebruik BSN;
- Artikel 35: gebruik bijzondere en strafrechtelijke gegevens;
- Artikel 37: gebruik van gegevens, geen verdere vertrekking en onherleidbare publicatie;
- Artikel 38: technische en organisatorische voorzieningen ter beveiliging van gegevens;
- Artikel 39 - 42: verstrekken van gegevens ten behoeve van statistisch onderzoek (Remote Acces).

De Ambtenarenwet 2017
Artikel 5 en 9 van de Ambtenarenwet 2017.

Bijlage 2. Begrippen en definities

AVG: Algemene verordening gegevensbescherming; Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming).

Betrokkene: een geïdentificeerde of identificeerbare natuurlijke persoon; degene op wie een persoonsgegeven betrekking heeft.

Bijzondere persoonsgegevens: persoonsgegevens waaruit ras of etnische afkomst, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen, of het lidmaatschap van een vakbond blijken, en genetische gegevens, biometrische gegevens met het oog op de unieke identificatie van een persoon, of gegevens over gezondheid, of gegevens met betrekking tot iemands seksueel gedrag of seksuele gerichtheid.

Strafrechtelijke persoonsgegevens: persoonsgegevens betreffende strafrechtelijke veroordelingen en strafbare feiten of daarmee verband houdende veiligheidsmaatregelen.

CISO: Chief Information Security Officer.

CQO: Chief Quality Officer.

CPO: Chief Privacy Officer.

Datalek: een inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens.

DPIA: Data Protection Impact Assessment.

FG: Functionaris Gegevensbescherming.

Onrechtmatige verwerking van gegevens: verwerking van persoonsgegevens zonder geldige wettelijke grondslag.

Persoonsgegeven: alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon (de betrokkene). Als identificeerbaar wordt beschouwd een natuurlijke persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identificator zoals een naam, een identificatienummer, locatiegegevens, een online identificator of van een of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon. Ook versleutelde of gepseudonimiseerde gegevens zijn persoonsgegevens. Denk naast Naam of BSN ook aan een kenteken, of een IP adres.

Privacy by design: ontwerpfilosofie die vereist dat privacybescherming vanaf het begin af aan meegenomen wordt bij het ontwerpen en bouwen van nieuwe systemen.

Privacy by default: standaardinstellingen zijn altijd zo privacy-vriendelijk mogelijk.

Proportionaliteit: het doel van de verwerking van de persoonsgegevens staat in verhouding tot de inbreuk op de privacy van de betrokkene.

Pseudonimiseren: het verwerken van persoonsgegevens op zodanige wijze dat de persoonsgegevens niet meer aan een specifieke betrokkene kunnen worden gekoppeld zonder dat er aanvullende gegevens worden gebruikt, mits deze aanvullende gegevens apart worden bewaard en technische en organisatorische maatregelen worden genomen om ervoor te zorgen dat de persoonsgegevens niet aan een geïdentificeerde of identificeerbare natuurlijke persoon worden gekoppeld.

Subsidiariteit: er moet altijd gekeken worden of het beoogde doel ook op een minder ingrijpende manier en/ of met minder ingrijpende middelen kan worden bereikt.

Toezichthouder: de autoriteit die verantwoordelijk is voor het handhaven van de bescherming van persoonsgegevens (AVG en UAVG). In Nederland is dit de Autoriteit Persoonsgegevens.

Verwerkingsverantwoordelijke: een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat, alleen of samen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt. In geval van CBS is dit de directeur-generaal van de statistiek.

Verwerking: een bewerking of een geheel van bewerkingen met betrekking tot persoonsgegevens of een geheel van persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedés, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van gegevens.

Verwerker: een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat ten behoeve van de verwerkingsverantwoordelijke persoonsgegevens verwerkt.