bijlage

Regels voor het gebruik van de Remote Access-faciliteit van het CBS

(versie maart 2017)

1. **Respecteer altijd de vertrouwelijkheid van de gegevens die aan u ter beschikking zijn gesteld.**

   De bestanden waarmee u werkt bevatten gevoelige gegevens over personen, huishoudens of bedrijven. De uitkomsten van uw onderzoek mogen onder geen enkele voorwaarde herleidbaar zijn tot personen, huishoudens, ondernemingen of instellingen. Dit impliceert tevens dat de gegevens niet gebruikt kunnen worden voor handhaving of administratieve correcties.

2. **Ga zorgvuldig om met uw token en deel uw token en wachtwoord met niemand.**

   Uw token en wachtwoord zijn persoonlijk en mogen niet gedeeld worden. Meld diefstal/verlies van of schade aan uw token direct aan het CBS.

3. **Laat geen onbevoegden meekijken op uw pc-scherm als u toegang heeft tot het Remote Access-netwerk.**

   Iedereen die mee kan kijken op uw pc-scherm dient in het bezit te zijn van een geldige CBS geheimhoudingsverklaring. U mag dus niet in een openbare ruimte verbinding maken met het Remote Access-netwerk.

4. **Zorg dat de pc waarop u werkt op het Remote Access-netwerk goed beveiligd is en zet bij het verlaten van de pc altijd de screensaver aan of verbreek de verbinding met het CBS.**

   Zorg dat u werkt op een beveiligd netwerk met goed bijgewerkte antivirussoftware. Het is niet toegestaan om te werken op een openbaar toegankelijk wifi netwerk. Zorg ervoor dat de screensaver met een wachtwoord is beveiligd.

5. **Gebruik de informatie uit de microdata alleen voor het onderzoeksproject dat u vooraf bij het CBS heeft ingediend.**

   U krijgt toegang tot bestanden voor een specifiek onderzoeksproject, waarbij wij controleren of de aangevraagde bestanden inderdaad nodig zijn voor het beantwoorden van de onderzoeksvragen binnen het project. In dat kader moet voor elk onderzoeksproject de doelbinding van de aangevraagde bestanden opnieuw worden beoordeeld. Voor een nieuw onderzoek moet dan ook altijd opnieuw toegang gevraagd worden. Microdata kunnen nooit gebruikt worden voor handhaving of administratieve correcties.

6. **U mag op geen enkele wijze gegevens van het scherm kopiëren.**

   U mag de gegevens beslist niet overschrijven, fotograferen of met behulp van de functieknop 'printscreen' buiten de Remote Access omgeving brengen. Ook als u inhoudelijke vragen heeft over de data, mag u niets overschrijven van het scherm en naar het CBS mailen, gebruik dan de juiste exportmap.

7. **Alle informatie die u vanuit de Remote Access-omgeving wilt exporteren plaatst u in de exportmap in uw account zodat medewerkers van het CBS deze kunnen controleren op onthullingsrisico.**

   U mag uw resultaten pas delen met anderen als het CBS de output veilig heeft bevonden, ook als uw output achteraf gecontroleerd wordt. Achteraf gecontroleerde output mag in de tussentijd wel gedeeld worden met anderen binnen uw instelling die in het bezit zijn van een CBS geheimhoudingsverklaring. Als achteraf gecontroleerde output niet veilig wordt bevonden, dient u deze meteen te vernietigen. U bent medeverantwoordelijk dat er geen onthullende informatie buiten de Remote Access-omgeving gebracht wordt.

8. **U bent verplicht de resultaten van uw onderzoek openbaar te publiceren.**

   Stuur een kopie van uw publicatie op naar ***microdata@cbs.nl****. Wij plaatsen de referentie dan op onze website.*

9. **Draai niet meer dan twee applicatiesessies tegelijk (fair use).**

   De CBS Microdata-infrastructuur is ingericht voor maximaal twee gelijktijdige sessies per gebruiker. Als gebruikers gelijktijdig meerdere sessies naar statistische applicaties open hebben staan, kan de belasting op de server infrastructuur te hoog worden en kunnen u en andere gebruikers hier last van ondervinden.

10. **Neem contact op met het CBS bij vragen of twijfel over bovenstaande regels.**

    Microdataservices is telefonisch of via email bereikbaar op werkdagen van 8:30 tot 17:00 uur. Via de mail op ***microdata@cbs.nl*** *of telefonisch op 088-5707070.*