Microdata Services – Remote Access Sanctioning Policy

	Description	Sanction[1]
Minor breach	If an action by the Remote Access (RA) user leads to an incident, this is a minor breach. An ***incident*** is a disturbing event or circumstance that may cause disruption of Statistics Netherlands' (hereinafter CBS) processes. The following is considered an incident in any case: 1. Failure to report the missing, loss or theft of: a. RA username and/or password; b. a phone that has been registered with CBS for the RA SMS code; c. RA token provided by CBS. 2. Lending of the RA token.	Warning letter to the supervisor of the researcher(s) and revocation of the privilege to post-check for the entire project for a period of up to six months. The breach shall be recorded for 3 years. If a new incident is reported within one year after the first incident in a project, these breaches shall be considered severe.
Severe breach	*A **security incident** is an incident which possibly violates the confidentiality, integrity or availability of data available within CBS.* The following breaches are considered severe in any case: 1. Bypassing the output control by copying, photographing etc. of RA aggregated data from the monitor. 2. Working in a public space. 3. Working on a computer which connects to the Remote Access via a public WiFi network (for example on trains, in cafes etc.). 4. Letting an unauthorised person work in the RA environment. 5. Otherwise violating the confidentiality of the data provided.	Revocation of login rights of the researcher involved for a period of up to one month as well as revocation of the privilege to post-check for the entire project for a period of up to six months, depending on the severeness of the breach and the intensity of the use of RA facilities. The organisation of the researcher(s) must take measures to prevent recurrence. The breach shall be recorded for 3 years. If more than one severe breach is reported within one year after completion or within 3 years during the project, these shall be considered very severe.
Very severe breach	A ***data leak*** is a security incident in which *personal or business data* have been lost or in which it cannot reasonably be ruled out that personal or business data were processed unlawfully (a full definition can be found on the website of the Dutch Data Protection Authority (Autoriteit	Suspension of the project agreement for <u>all</u> researchers involved for a period of at least 6 months up to 1 year, depending on the severeness of the breach and the intensity

[1] Any appeals against this decision shall be submitted within six weeks from the date of dispatch of the sanction letter by persons directly affected by the decision. These can be sent to: The Director General of Statistics, c/o Statistics Netherlands, PO Box 24500, 2490 HA The Hague, the Netherlands.
The type of sanction and its duration will be determined on the basis of incriminating evidence by the director of SDI (Statistical Services and Information) and the head of Microdata Services.

	Persoonsgegevens). The following breaches are considered very severe in any case: 1. Bypassing the output control by copying, photographing etc. of RA *personal or business data* from the monitor. 2. Not destroying the output if post-checks indicate that the output still is not safe. Or: 3. Otherwise causing or contributing to a data leak.	of the use of RA facilities. All tokens of researchers involved are deactivated during the suspension period. After the suspension period, the organisation may re-submit a request with CBS for restarting the project. Whether the project agreement is restarted by CBS also depends on the measures taken by the organisation to prevent recurrence. The breach shall be recorded for 3 years.