**SOP Template – Back up, archiving and deletion of your sensitive data**

Data Protection Quick Wins project

***Date of publication :*** *December 2017*

***Author :*** *Quality and Accountability unit*

The aim of this SOP is to define the procedures for delegations concerning the life cycle of their sensitive data. This template needs to be adapted by the delegation based on their contextual needs.

1. ***BACKUP OF YOUR SENSITIVE DATA***

The Backup of your dataset should be done every XX days / weeks (to adapt to your context / the database in question) and should be done on an external drive and a OneDrive folder (to adapt to your context / the database in question).

You will need to make sure that the data is not available on any non-protected location.

*Please refer to the “****2.11. How to archive and back-up your data****” tutorial to know how more.*

1. ***ARCHIVING YOUR SENSITIVE DATA***

The project data being archived is the following: full dataset / reduced dataset of [name of the project] (to adapt to the data protection risks identified for the database in question)

The archiving of your data should be done (to adapt to your context / the database in question):

On a relevant OneDrive folder

On the delegation’s secure external drive

The roles in the organisation having access to the archive are the following: XX (to adapt to your context/ the database in question).

*Please refer to the “****2.11. How to archive and back-up your data****” tutorial to know how more.*

1. ***DELETING DEFINITIVELY SENSITIVE DATA***

When handling a sensitive dataset, it is recommended to do the following actions:

* + - 1. Deleting definitively sensitive data from a computer:

- Use CCleaner on a regular basis (every X weeks) (to adapt to your context/ the database in question) to remove temporary files

- Use Eraser on the database file itself to delete all the traces left completely once you have it stored in a safe location

* + - 1. Deleting definitively sensitive data from a mobile device:

If you are using mobile data collection, you should activate encryption on the app you are using so that the data does not even need to be deleted but will never be exploitable by anyone.

If you are for any reason collecting data that is not encrypted on your mobile, use Undeleter on the data itself *(to detail)*

*Please refer to the “****2.10. How to permanently delete data from your device****” tutorial to know how more.*