EUROPEAN
COMMISSION

Brussels, XXX
[…](2024) XXX draft

ANNEX

ANNEX

to the

Delegated Regulation

supplementing Regulation (EU) 2022/2065 of the European Parliament and of the Council by laying down the technical conditions and procedures under which providers of very large online platforms and very large online search engines are to share data pursuant to Article 40 of Regulation (EU) 2022/2065

ANNEX

Responsibilities of the Commission as processor for data processing activities conducted in the context of the DSA data access portal

1. The Commission shall:

   (a) set up and ensure a secure and reliable IT infrastructure, the DSA data access portal, on behalf of the Digital Services Coordinators, that supports and streamlines the management of the data access process for researchers, research organisations, data providers and Digital Services Coordinators, and;

   (b) process personal data only based on documented instructions from the controllers.

2. To fulfil its obligations as processor for the Digital Services Coordinators, the Commission may use third parties as sub-processors. If it is the case, the controllers shall authorise the Commission to use sub-processors or replace sub-processors where necessary. The Commission shall inform the controllers of said use or replacement of sub-processors, thereby giving the controllers the opportunity to object to any such changes. The Commission shall ensure that the same data protection obligations as set out in this Regulation apply to these sub-processors.

3. The processing by the Commission shall entail:

   (a) authentication and access control with regard to all DSA data access portal users;

   (b) authorisation implementation of requests by DSA data access portal users to create, update and delete any information contained in the application within the DSA data access portal;

   (c) reception of the personal data referred to in Article xx of this Regulation uploaded by DSA data access portal users;

   (d) storage of the personal data in the DSA data access portal;

   (e) deletion of the personal data at their expiration date or upon instruction of the controller;

   (f) after the end of the provision of service, deletion of any remaining personal data unless Union or Member State laws require storage of such personal data.

4. The Commission shall take all state of the art organisational, physical, and logical security measures to ensure the DSA data access portal functioning. To this end, the Commission shall:

   (a) designate a responsible entity for the security management of the DSA data access portal, communicate to the controllers its contact information and ensure its availability to react to security threats;

   (b) assume the responsibility for the security of the DSA data access portal, including regularly carrying out tests, evaluations and assessments of the security measures;

5. The Commission shall take all necessary security measures to avoid compromising the smooth operational functioning of the DSA data access portal. This shall include:

(a) risk assessment procedures to identify and estimate potential threats to the DSA data access portal;

(b) audit and review procedure to:

(a) check the correspondence between the implemented security measures and the applicable security policy;

(b) control on a regular basis the integrity of the DSA data access portal, security parameters and granted authorisations;

(c) detect security breached and intrusions into the DSA data access portal;

(d) implement changes to mitigate existing security weaknesses in the DSA data access portal;

(e) define the conditions under which to authorise, including at the request of controllers, and contribute to, the performance of independent audits, including inspections, and reviews on security measures subject to conditions that respect Protocol (No 7) to the Treaty on the Functioning of the European Union on the Privileges and Immunities of the European Union;

(c) changing the control procedure to document, measure the impact of a change before its implementation, and keep the controllers informed of any changes that can affect the communication with and/or the security of the DSA data access portal;

(d) laying down a maintenance and repair procedure to specify the rules and conditions to be respected when maintenance and/or repair of the DSA data access portal is to be performed;

(e) laying down a security incident procedure to define the reporting and escalation scheme, inform without delay the controllers affected, inform without delay the controllers for them to notify the national data protection supervisory authorities of any personal data breach and define a disciplinary process to deal with security breaches in the DSA data access portal.

6. The Commission shall take state of the art physical and logical security measures for the facilities hosting the DSA data access portal and for the controls of data and security access thereto. To this end, the Commission shall:

(a) enforce physical security to establish distinct security perimeters and allowing detection of breaches in the DSA data access portal;

(b) control access to the DSA data access portal facilities;

(c) ensure that equipment cannot be added, replaced or removed without prior authorisation from the designated responsible bodies;

(d) control access from and to the DSA data access portal;

(e) ensure that the DSA data access portal users who access the DSA data access portal are authenticated;

(f) review the authorisation rights related to the access to the DSA data access portal in case of a security breach affecting the DSA data access portal;

(g) keep the integrity of the information transmitted through the DSA data access portal;

(h) implement technical and organisational security measures to prevent unauthorised access to personal data in the DSA data access portal;

(i) implement, whenever necessary, measures to block unauthorised access to the DSA data access portal (i.e., block a location/IP address).

7. The Commission shall:

(a) take steps to protect its domain, including the severing of connections, in the event of substantial deviation from the principles and concepts for quality and security;

(b) maintain a risk management plan related to its area of responsibility;

(c) monitor, in real time, the performance of all the service components of the DSA data access portal, produce regular statistics and keep records;

(d) provide support for the DSA data access portal in English to the DSA data access portal users;

(e) assist the controllers by appropriate technical and organisational measures for the fulfilment of the controller's obligation to respond to requests for exercising the data subject's rights laid down in Chapter III of Regulation (EU) 2016/679;

(f) support the controllers by providing information concerning the DSA data access portal to implement the obligations pursuant to Articles 32, 33, 34, 35 and 36 of Regulation (EU) 2016/679;

(g) ensure that data processed within the DSA data access portal is unintelligible to any person who is not authorised to access it;

(h) take all relevant measures to prevent unauthorised access to transmitted personal data via the DSA data access portal;

(i) take measures in order to facilitate communication between the controllers;

(j) maintain a record of processing activities carried out on behalf of the controllers in accordance with Article 31(2) of Regulation (EU) 2018/1725.