EUROPEAN COMMISSION
DIRECTORATE-GENERAL FOR
INFORMATICS

[redacted]

SERVICE LEVEL AGREEMENT (SLA) DIGIT-017-00

between

THE EUROPEAN DATA PROTECTION SUPERVISOR (EDPS)

and

THE DIRECTORATE-GENERAL FOR INFORMATICS OF THE EUROPEAN COMMISSION (DG DIGIT)

Ref: SLA DIGIT-017-03

The European Data protection Supervisor , hereinafter called "EDPS", represented for the conclusion of this amendment by [redacted]

And

the Directorate-General for Informatics, hereinafter "DIGIT", represented by [redacted]

(hereinafter jointly referred to as 'the parties')

Have agreed as follows

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

For DG DIGIT,

[redacted]

[e-signed]

[e-signed]

EUROPEAN COMMISSION

DIRECTORATE-GENERAL FOR INFORMATICS

APPENDIX A-9

To SLA No. DIGIT -017-03

DIGIT.B.4.002 - Management Support Services

Service: Confluence platform

[redacted]

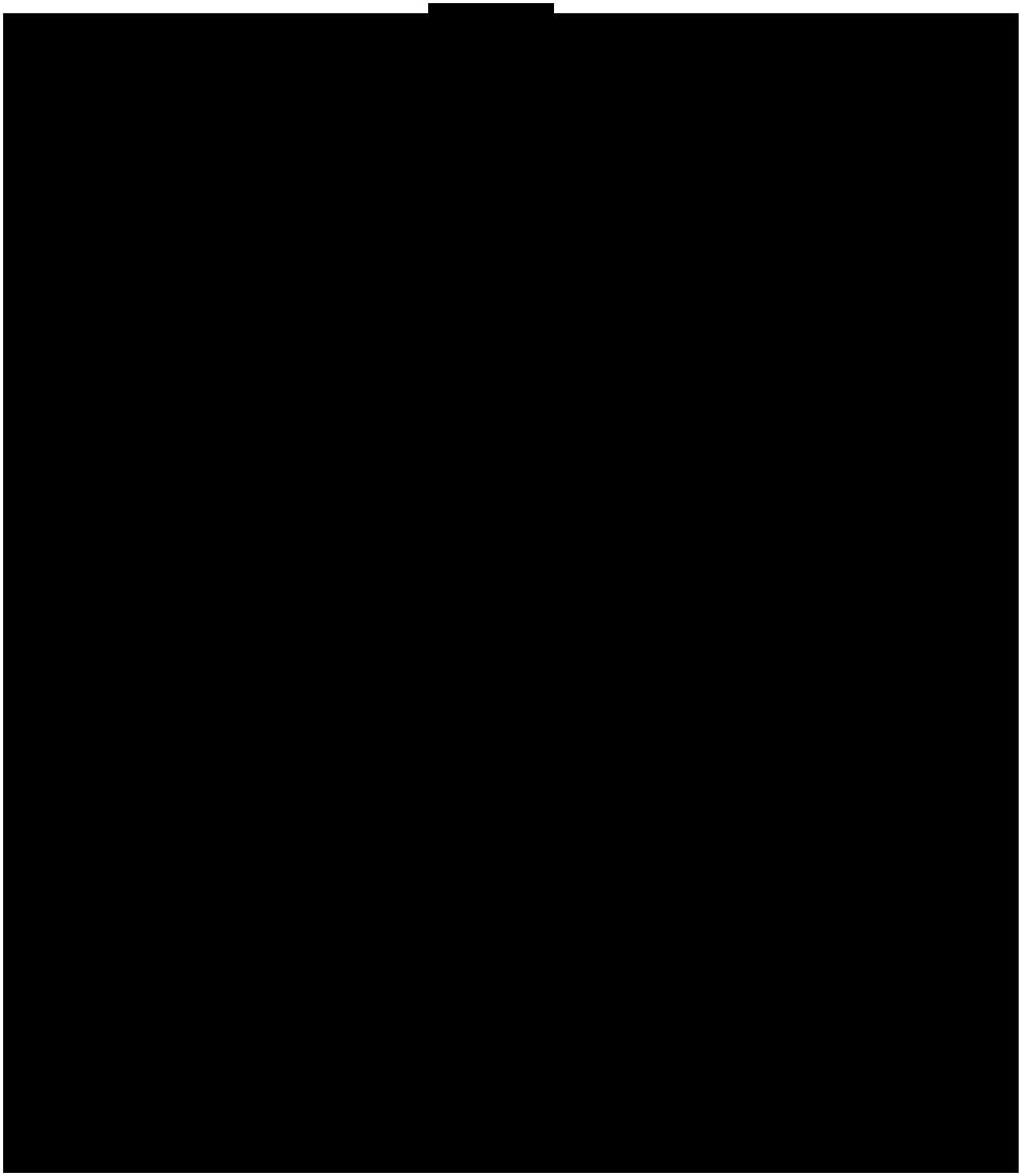
Article 1

Scope of the service

1. The aim of this Appendix is to define the conditions under which Directorate-General for Informatics of the European Commission (the service provider) renders to the customer EUI (the client) the service "**Confluence platform**" (the Service/the Services), according to the description provided in this appendix.

2. The provision of the service shall be governed by the provisions of the Service Level Agreement SLA [redacted]

[redacted]



[redacted]

Article 8

Specific Security and Data Protection Arrangements

As stipulated in point 3 of article 13 of the SLA, if the processing operation involves the processing of personal data, the parties agree that the service provider acts as a processor for the client, who acts as controller. As a result, the specific provisions pertaining to the processing of personal data, and to the relationship between controller and processor, are detailed in this article.

The processing of personal data by the processor shall meet the requirements of Regulation (EU) 2018/1725 and be processed solely for the purposes set out by the controller.[2]

The subject matter and purpose of the processing of personal data by the processor is to assist the controller in ensuring the performance of the tasks of the EDPB, including its Secretariat, stipulated in article 75(6) of Regulation 2016/679 (henceforth "GDPR").[3] This includes the processing of personal data for platform management.

The localisation of, and access to the personal data processed by the processor shall comply with the following:

i. the personal data shall only be processed within the territory of the European Union and the European Economic Area and will not leave that territory;
ii. the data shall only be held in data centres located with the territory of the European Union and the European Economic Area;
iii. access to data may be given on a need to know basis only to authorised persons established in a country which has been recognised by the European Commission as providing adequate protection to personal data;
the processor may not change the location of data processing without the prior written authorisation of the EDPS. In this case, any transfer of personal data under the contract to third countries or international organisations shall fully comply with the requirements laid down in Chapter V of Regulation (EU) 2018/1725.

The categories of data subjects involved in this processing operation include staff members of EDPB (including members and observers), staff members of the EDPS, including from the EDPB Secretariat and staff members of the European Commission. Documents and specific sets of information uploaded in Confluence may also contain personal data of parties and/or individuals who are external to the EDPB, its Members and the European Commission.

The processed categories of personal data include: username, name and surname of the user, professional email address, office phone number, pictures, professional affiliation and country, as well as any views, opinions or documents made available in Confluence that can lead to the individual's direct or indirect identification. In addition, the service provider processes user logs and IP addresses of users, in order to ensure the management and security of the platform.

The processor may only process personal data on documented written instructions and under the supervision of the controller, in particular with regard to the purposes of the processing, the categories of data that may be processed, the recipients of the data and the means by which the data subject may exercise its rights.

---

[2] Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC, OJ L 295, 21.11.2018, p. 39–98

[3] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119, 4.5.2016, p. 1–88

The processor shall grant personnel access to the data to the extent strictly necessary for the implementation, management and monitoring of the contract. The processor must ensure that personnel authorised to process personal data has committed itself to confidentiality or is under appropriate statutory obligation of confidentiality.

The processor shall adopt appropriate technical and organisational security measures, giving due regard to the risks inherent in the processing and to the nature, scope, context and purposes of processing, in order to ensure, in particular, as appropriate:

(a) the pseudonymisation and encryption of personal data;
(b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
(c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
(d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing;
(e) measures to protect personal data from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access to personal data transmitted, stored or otherwise processed.

The processor shall notify relevant personal data breaches to the controller without undue delay and at the latest within 48 hours after the processor becomes aware of the breach. In such cases, the processor shall provide the controller with at least the following information:

(a) nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;
(b) likely consequences of the breach;
(c) measures taken or proposed to be taken to address the breach, including, where appropriate, measures to mitigate its possible adverse effects.

The processor shall immediately inform the data controller if, in its opinion, an instruction infringes Regulation (EU) 2018/1725, or Regulation (EU) 2016/679.

The processor shall assist the controller for the fulfilment of the controller's obligation to respond to requests for exercising rights of persons whose personal data is processed in relation to this contract as laid down in Chapter III (Articles 14-25) of Regulation (EU) 2018/1725. The processor shall inform without delay the controller about such requests.

The processor shall also assist the controller for the fulfilment of its obligations pursuant to Article 33 to 41 under Regulation (EU) 2018/1725 to:

(a) ensure compliance with its data protection obligations regarding the security of the processing, and the confidentiality of electronic communications and directories of users;
(b) notify a personal data breach to the European Data Protection Supervisor;
(c) communicate a personal data breach without undue delay to the data subject, where applicable;
(d) carry out data protection impact assessments and prior consultations as necessary.

The processor shall maintain a record of all data processing operations carried on behalf of the controller, transfers of personal data, security breaches, responses to requests for exercising rights of people whose personal data is processed and requests for access to personal data by third parties.

The processor shall notify the EDPS without delay of any legally binding request for disclosure of the personal data processed on behalf of the EDPS made by any national public authority, including an authority from a third country. The processor may not give such access without the prior written authorisation of the EDPS.

The duration of processing of personal data by the processor will not exceed the duration period of the service provision, referred to in Article 2. Upon expiry of this period, the processor shall, at the choice of the controller, return, without any undue delay in a commonly agreed format, all personal data processed on behalf of the controller and the copies thereof or shall effectively delete all personal data unless Union or national law requires a longer storage of personal data.

The processor shall not engage another processor without prior specific authorisation of the EDPS. If part, or all of the processing of personal data, is subcontracted to a subcontractor, , the processor shall pass on the obligations referred to in this article, in writing, to those subcontractors. At the request of the EDPS, the processor shall provide a document providing evidence of this commitment. Where subcontractors fails to fulfil its data protection obligations, the initial processor shall remain fully liable to the controller for the performance of that other processor's obligations.