►**B**

COMMISSION IMPLEMENTING DECISION 2019/1765

of 22 October 2019

providing the rules for the establishment, the management and the functioning of the network of national authorities responsible for eHealth, and repealing Implementing Decision 2011/890/EU

(notified under document C(2019) 7460)

(Text with EEA relevance)

(OJ L 270, 24.10.2019, p. 83)

Amended by:

		Official Journal		
		No	page	date
►**M1**	Commission Implementing Decision (EU) 2020/1023 of 15 July 2020	L 227 I	1	16.7.2020

▼B

COMMISSION IMPLEMENTING DECISION 2019/1765

of 22 October 2019

providing the rules for the establishment, the management and the functioning of the network of national authorities responsible for eHealth, and repealing Implementing Decision 2011/890/EU

(notified under document C(2019) 7460)

(Text with EEA relevance)

Article 1

Subject matter

This Decision provides the necessary rules for the establishment, the management and the functioning of the eHealth Network of national authorities responsible for eHealth, as provided for by Article 14 of Directive 2011/24/EU.

Article 2

Definitions

1. For the purposes of this Decision:

(a) ‘eHealth Network’ means the voluntary network connecting national authorities responsible for eHealth designated by the Member States and pursuing the objectives laid down in Article 14 of Directive 2011/24/EU;

(b) ‘National Contact Points for eHealth’ means organisational and technical gateways for the provision of Cross-Border eHealth Information Services under the responsibility of the Member States;

(c) ‘Cross-Border eHealth Information Services’ means existing services that are processed via National Contact Points for eHealth and through a core service platform developed by the Commission for the purpose of cross-border healthcare;

(d) ‘eHealth Digital Service Infrastructure for Cross-Border eHealth Information Services’ means the infrastructure that enables the provision of Cross-Border eHealth Information Services via National Contact Points for eHealth and the European core service platform. This infrastructure includes both generic services, as defined in Article 2(2)(e) of Regulation (EU) No 283/2014, developed by the Member States and a core service platform, as defined in Article 2(2)(d) therein, developed by the Commission;

(e) ‘other shared European eHealth Services’ means digital services that may be developed in the framework of the eHealth Network and shared between Member States;

▼B

(f) ‘governance model’ means a set of rules concerning the designation of bodies participating in decision-making processes concerning the eHealth Digital Service Infrastructure for Cross-Border eHealth Information Services or other shared European eHealth Services developed in the framework of the eHealth Network, as well as description of those processes;

▼M1

(g) ‘application user’ means a person in possession of a smart device who has downloaded and runs an approved contact tracing and warning mobile application;

(h) ‘contact tracing’ means measures implemented in order to trace persons who have been exposed to a source of a serious cross-border threat to health within the meaning of Article 3(c) of Decision No 1082/2013/EU of the European Parliament and of the Council ([1]);

(i) ‘national contact tracing and warning mobile application’ means a software application approved at national level running on smart devices, in particular smartphones, designed usually for wide-ranging and targeted interaction with web resources, which processes proximity data and other contextual information collected by many sensors found in the smart devices for the purpose of tracing contacts with persons infected with SARS-CoV-2 and alerting persons who may have been exposed to SARS-CoV-2. These mobile applications are able to detect the presence of other devices using Bluetooth and exchange information with backend servers by using the internet;

(j) ‘federation gateway’ means a network gateway operated by the Commission through a secure IT tool that receives, stores and makes available a minimum set of personal data between Member States’ backend servers for the purpose of ensuring the interoperability of national contact tracing and warning mobile applications;

(k) ‘key’ means a unique ephemeral identifier related to an application user reporting to have been infected with SARS-CoV-2, or who may have been exposed to SARS-CoV-2;

(l) ‘verification of infection’ means the method applied for confirming an infection with SARS-CoV-2, namely whether this was self-reported by the application user or resulted from confirmation from a national health authority or a laboratory test;

(m) ‘countries of interest’ means the Member State, or Member States, where an application user has been in the 14 days prior to the date of upload of the keys and where he has downloaded the approved national contact tracing and warning mobile application and/or has travelled;

([1]) Decision No 1082/2013/EU of the European Parliament and of the Council of 22 October 2013 on serious cross-border threats to health and repealing Decision No 2119/98/EC (OJ L 293, 5.11.2013, p. 1).

▼M1

(n) ‘country of origin of the keys’ means the Member State where the backend server that uploaded the keys to the federation gateway is located;

(o) ‘log data’ means an automatic record of an activity in relation to the exchange of, and access to, data processed through the federation gateway, that show in particular the type of processing activity, the date and time of the processing activity, and the identifier of the person processing the data.

▼B

2. The definitions in points (1), (2), (7) and (8) of Article 4 of Regulation (EU) 2016/679 shall apply accordingly.

Article 3

Membership of the eHealth Network

1. Members of the eHealth Network shall be Member States’ authorities responsible for eHealth, designated by those Member States participating in the eHealth Network.

2. Member States wishing to participate in the eHealth Network shall notify the Commission in writing of:

(a) the decision to participate in the eHealth Network;

(b) the national authority responsible for eHealth which will become a Member of the eHealth Network, as well as the name of the representative and that of his/her alternate.

3. Members shall notify the Commission in writing of the following:

(a) their decision to withdraw from the eHealth Network;

(b) any change in the information referred to in point (b) of paragraph 2.

4. The Commission shall make available to the public the list of Members participating in the eHealth Network.

Article 4

Activities of the eHealth Network

1. In pursuing the objective referred to in Article 14(2)(a) of Directive 2011/24/EU the eHealth Network may, in particular:

(a) facilitate greater interoperability of the national information and communications technology systems and cross-border transferability of electronic health data in cross-border healthcare;

(b) provide guidance to Member States, in cooperation with other competent supervisory authorities, in relation to sharing health data between Member States and empowering citizens to access and share their own health data;

▼B

(c) provide guidance to Member States and facilitate the exchange of good practices concerning the development of different digital health services, such as telemedicine, m-health, or new technologies in the area of big data and artificial intelligence, taking into consideration ongoing actions at EU level;

(d) provide guidance to Member States as regards supporting health promotion, disease prevention and improved delivery of healthcare through better use of health data and by improving digital skills of patients and healthcare professionals;

(e) provide guidance to Member States and facilitate voluntary exchange of best practices on the investments in digital infrastructure;

(f) provide guidance, in collaboration with other relevant bodies and stakeholders, to Member States on the necessary use cases for clinical interoperability and the tools for achieving it;

(g) provide guidance to the Members on security of the eHealth Digital Service Infrastructure for Cross-Border eHealth Information Services or other shared European eHealth Services developed in the framework of the eHealth Network, taking into account legislation and documents elaborated at Union level in particular in the area of security, as well as recommendations in the field of cybersecurity, working in close cooperation with the Network and Information Security Cooperation Group and with the European Union Agency for Network and Information Security and with national authorities, where relevant;

▼M1

(h) provide guidance to the Member States on the cross-border exchange of personal data through the federation gateway between national contact tracing and warning mobile applications.

▼B

2. In drawing up the guidelines on effective methods for enabling the use of medical information for public health and research referred to in Article 14(2)(b)(ii) of Directive 2011/24/EU, the eHealth Network shall take into account the guidelines adopted by and, where appropriate, consult with the European Data Protection Board. These guidelines may also address information exchanged through the eHealth Digital Service Infrastructure for Cross-Border eHealth Information Services or other shared European eHealth Services.

Article 5

Functioning of the eHealth Network

1. The eHealth Network shall establish its own Rules of Procedure, by simple majority of its Members.

2. The eHealth Network shall adopt a multiannual work programme and an evaluation instrument on the implementation of such programme.

▼B

3. To accomplish its tasks, the eHealth Network may set up permanent subgroups in relation to specific tasks, in particular related to the eHealth Digital Service Infrastructure for Cross-Border eHealth Information Services or the other shared European eHealth Services developed in the framework of the eHealth Network.

4. The eHealth Network may also set up temporary sub-groups, including with experts to examine specific questions on the basis of terms of reference defined by the eHealth Network itself. Such sub-groups shall be disbanded as soon as their mandate is fulfilled.

5. When Members of the eHealth Network decide to advance their cooperation in some areas covered by the tasks of the eHealth Network, they should agree on and commit to the rules of the advanced cooperation.

6. In pursuing its objectives, the eHealth Network shall work in close cooperation with the Joint Actions supporting the activities of the eHealth Network where such joint actions exist, with stakeholders or other concerned bodies or supporting mechanisms and shall take into account the results achieved in the framework of those activities.

7. The eHealth Network shall elaborate, together with the Commission, the governance models of the eHealth Digital Service Infrastructure for Cross-Border eHealth Information Services and participate in that governance by:

(i) agreeing on the priorities of the eHealth Digital Service Infrastructure, and overseeing their operation;

(ii) drawing up guidelines and requirements for the operation, including the selection of the standards used for the eHealth Digital Service Infrastructure for Cross-Border eHealth Information Services;

(iii) agreeing whether the Members of the eHealth Network should be allowed to start and continue exchanging electronic health data through the eHealth Digital Service Infrastructure for Cross-Border eHealth Information Services via their National Contact Points for eHealth, based on their compliance with the requirements established by the eHealth Network, as evaluated in tests provided and audits carried out by the Commission;

(iv) endorsing the annual work plan for the eHealth Digital Service3 Infrastructure for Cross-Border eHealth Information Services.

8. The eHealth Network may elaborate, together with the Commission, the governance models of other shared European eHealth Services developed in the framework of the eHealth Network and participate in their governance. The Network may also set the priorities, together with the Commission, and draw up guidelines for the operation of such shared European eHealth Services.

▼B

9. The Rules of Procedure may envisage that countries, other than Member States, applying Directive 2011/24/EU, may participate in the meetings of the eHealth Network as observers.

10. Members of the eHealth Network and their representatives, as well as invited experts and observers, shall comply with the obligations of professional secrecy as laid down by Article 339 of the Treaty, as well as with the Commission's rules on security regarding the protection of EU classified information, as laid down in Commission Decision (EU, Euratom) 2015/444 ([1]). Should they fail to respect these obligations, the Chair of the eHealth Network may take all appropriate measures as provided for in the Rules of Procedure.

Article 6

Relation between the eHealth Network and the Commission

1. The Commission shall:

(a) attend and co-chair the meetings of the eHealth Network together with the representative of the Members;

(b) cooperate with and provide support to the eHealth Network in relation to its activities;

(c) provide secretarial services for the eHealth Network;

(d) develop, implement and maintain appropriate technical and organisational measures related to the core services of the eHealth Digital Service Infrastructure for Cross-Border eHealth Information Services;

(e) support the eHealth Network in agreeing on the technical and organisational compliance of National Contact Points for eHealth with the requirements for the cross-border exchange of health data by providing and carrying out the necessary tests and audits. Experts from the Member States may assist Commission auditors;

▼M1

(f) develop, implement and maintain appropriate technical and organisational measures related to the security of transmission and hosting of personal data in the federation gateway for the purpose of ensuring the interoperability of national contact tracing and warning mobile applications;

(g) support the eHealth Network in agreeing on the technical and organisational compliance of the national authorities with the requirements for the cross-border exchange of personal data in the federation gateway by providing and carrying out the necessary tests and audits. Experts from the Member States may assist the Commission auditors.

▼B

2. The Commission may attend the meetings of the eHealth Network sub-groups.

3. The Commission may consult the eHealth Network on matters relating to eHealth at Union level and eHealth best practices exchange.

([1]) Commission Decision (EU, Euratom) 2015/444 of 13 March 2015 on the security rules for protecting EU classified information (OJ L 72, 17.3.2015, p. 53).

▼B

4. The Commission shall make available to the public information on activities carried out by the eHealth Network.

Article 7

▼M1

Protection of personal data processed through the eHealth Digital Service Infrastructure

▼B

1. The Member States, represented by the relevant National Authorities or other designated bodies shall be regarded as controllers of personal data they process through the eHealth Digital Service Infrastructure for Cross-Border eHealth Information Services and shall clearly and transparently allocate the responsibilities between controllers.

2. The Commission shall be regarded as data processor for patients' personal data processed through the eHealth Digital Service Infrastructure for Cross-Border eHealth Information Services. In its capacity as processor, the Commission shall manage the core services of the eHealth Digital Service Infrastructure for Cross-Border eHealth Information Services and shall comply with the obligations of a processor laid down in the ►M1 Annex I ◄ to this Decision. The Commission shall not have access to patients' personal data processed through the eHealth Digital Service Infrastructure for Cross-Border eHealth Information Services.

3. The Commission shall be regarded as controller of the processing of personal data necessary to grant and manage access rights to the core services of eHealth Digital Service Infrastructure for Cross-Border eHealth Information Services. Such data are contact details of users, including name, surname and email address and their affiliation.

▼M1

Article 7a

Cross-border exchange of data between national contact tracing and warning mobile applications through the federation gateway

1. Where personal data is exchanged through the federation gateway, the processing shall be limited to the purposes of facilitating the interoperability of national contact tracing and warning mobile applications within the federation gateway and the continuity of contact tracing in a cross-border context.

2. The personal data referred to in paragraph 3 shall be transmitted to the federation gateway in a pseudonymised format.

▼M1

3. The pseudonymised personal data exchanged through and processed in the federation gateway shall only comprise the following information:

(a) the keys transmitted by the national contact tracing and warning mobile applications up to 14 days prior to the date of upload of the keys;

(b) log data associated to the keys in line with the technical specifications protocol used in the country of origin of the keys;

(c) the verification of infection;

(d) the countries of interest and the country of origin of the keys.

4. The designated national authorities or official bodies processing personal data in the federation gateway shall be joint controllers of the data processed in the federation gateway. The respective responsibilities of the joint controllers shall be allocated in accordance with Annex II. Each Member State wishing to participate in the cross-border exchange of data between national contact tracing and warning mobile applications shall notify the Commission, prior to joining, of its intention and indicate the national authority or official body that has been designated as the responsible controller.

5. The Commission shall be the processor of personal data processed within the federation gateway. In its capacity as processor, the Commission shall ensure the security of processing, including the transmission and hosting, of personal data within the federation gateway and shall comply with the obligations of a processor laid down in Annex III.

6. The effectiveness of the technical and organisational measures for ensuring the security of processing of personal data within the federation gateway shall be regularly tested, assessed and evaluated by the Commission and by the national authorities authorised to access the federation gateway.

7. Without prejudice to the decision of the joint controllers to terminate the processing in the federation gateway, the operation of the federation gateway shall be deactivated at the latest 14 days after all the connected national contact tracing and warning mobile applications cease to transmit keys through the federation gateway.

▼B

Article 8

Expenses

1. Participants in the activities of the eHealth Network shall not be remunerated by the Commission for their services.

▼B

2. Travel and subsistence expenses incurred by participants in the activities of the eHealth Network shall be reimbursed by the Commission in accordance with the provisions in force within the Commission on reimbursement of expenses incurred by people from outside the Commission invited to attend meetings in an expert capacity. Those expenses shall be reimbursed within the limits of the available appropriations allocated under the annual procedure for the allocation of resources.

Article 9

Repeal

Implementing Decision 2011/890/EU is repealed. References to the repealed Decision shall be construed as references to this Decision.

Article 10

Addressees

This Decision is addressed to the Member States.

▼M1

ANNEX I

▼B

RESPONSIBILITIES OF THE COMMISSION AS DATA PROCESSOR FOR THE EHEALTH DIGITAL SERVICE INFRASTRUCTURE FOR CROSS-BORDER EHEALTH INFORMATION SERVICES

The Commission shall:

1. Set up and ensure a secure and reliable communication infrastructure that interconnects networks of the Members of the eHealth Network involved in eHealth Digital Service Infrastructure for Cross-Border eHealth Information Services ('Central Secure Communication Infrastructure'). To fulfil its obligations, the Commission may engage third parties. The Commissions shall ensure that the same data protection obligations as set out in this Decision apply to these third parties.

2. Configure part of the Central Secure Communication Infrastructure so that the National Contact Points for eHealth may exchange information securely, reliably and efficiently.

3. The Commission shall process the personal data on documented instructions from the Controllers.

4. Take all organisational, physical and logical security measures to maintain the Central Secure Communication Infrastructure. To this end, the Commission shall:

   (a) designate a responsible entity for the security management at the level of Central Secure Communication Infrastructure, communicate to the data controllers its contact information and ensure its availability to react to security threats;

   (b) assume the responsibility for the security of the Central Secure Communication Infrastructure;

   (c) ensure that all individuals that are granted access to Central Secure Communication Infrastructure are subject to contractual, professional or statutory obligation of confidentiality;

   (d) ensure that the personnel having access to classified information fulfil the corresponding criteria of clearance and confidentiality.

5. Take all necessary security measures to avoid compromising the smooth operational functioning of the other's domain. To this end, the Commission shall put in place the specific procedures related to the connection to the Central Secure Communication Infrastructure. This information includes:

   (a) risk assessment procedure, to identify and estimate potential threats to the system;

   (b) audit and review procedure to:

      (i) check the correspondence between the implemented security measures and the security policy in application;

      (ii) control on a regular basis the integrity of system files, security parameters and granted authorisations;

      (iii) monitor to detect security breaches and intrusions;

      (iv) implement changes to avoid existing security weaknesses and

▼B

(v) 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.

(c) change control procedure to document and measure the impact of a change before its implementation and keep the National Contact Points for eHealth informed of any changes that can affect the communication with and/or the security of the other national infrastructures;

(d) maintenance and repair procedure to specify the rules and conditions to follow when maintenance and/or repair of equipment should be performed;

(e) security incident procedure to define the reporting and escalation scheme, inform without delay the responsible national administration, as well as the European Data Protection Supervisor of any security breach and define a disciplinary process to deal with security breaches.

6. Take physical and/or logical security measures for the facilities hosting the Central Secure Communication Infrastructure equipment and for the controls of logical data and security access. To this end, the Commission shall:

(a) enforce physical security to establish distinctive security perimeters and allowing detection of breaches;

(b) control access to the facilities and maintain a visitor register for tracing purposes;

(c) Ensure that external people granted access to premises are escorted by duly authorised staff of its respective organisation;

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

(e) control access from and to other network(s) interconnected to the Central Secure Communication Infrastructure;

(f) ensure that individuals who access the Central Secure Communication Infrastructure are identified and authenticated;

(g) review the authorisation rights related to the access to the Central Secure Communication Infrastructure in case a security breach affecting this infrastructure;

(h) keep the integrity of the transmitted information through the Central Secure Communication Infrastructure;

(i) implement technical and organisational security measures to prevent unauthorized access to personal data;

(j) implement, whenever necessary, measures to block unauthorised access to the Central Secure Communication Infrastructure from the domain of National Contact Points for eHealth (i.e.: Block a location/IP address).

7. Take steps to protect its domain, including the severing of connections, in the event of substantial deviation from the principles and concepts for quality or security.

8. Maintain a risk management plan related to its area of responsibility.

▼B

9. Monitor — in real time — the performance of all the service components of its Central Secure Communication Infrastructure services, produce regular statistics and keep records.

10. Provide support for all Central Secure Communication Infrastructure services in English 24/7 via phone, mail or Web Portal and accept calls from authorised callers: Central Secure Communication Infrastructure's coordinators and their respective helpdesks, Project Officers and designated people from the Commission.

11. Support the controllers by providing information concerning the Central Secure Communication Infrastructure of the eHealth Digital Service Infrastructure for Cross-Border eHealth Information Services, in order to implement the obligations in Articles 35 and 36 of the Regulation (EU) 2016/679.

12. Ensure that data transported within the Central Secure Communication Infrastructure are encrypted.

13. Take all relevant measures to prevent that the Central Secure Communication Infrastructure's operators have unauthorised access to transported data.

14. Take measures in order to facilitate the interoperability and the communication between the Central Secure Communication Infrastructure's designated national competent administrations.

▼M1

ANNEX II

RESPONSIBILITIES OF THE PARTICIPATING MEMBER STATES AS JOINT CONTROLLERS FOR THE FEDERATION GATEWAY FOR CROSS-BORDER PROCESSING BETWEEN NATIONAL CONTACT TRACING AND WARNING MOBILE APPLICATIONS

SECTION 1

Subsection 1

Division of responsibilities

(1) The joint controllers shall process personal data through the federation gateway in accordance with the technical specifications stipulated by the eHealth Network ([1]).

(2) Each controller shall be responsible for the processing of personal data in the federation gateway in accordance with the General Data Protection Regulation and Directive 2002/58/EC.

(3) Each controller shall set up a contact point with a functional mailbox that will serve for the communication between the joint controllers and between the joint controllers and the processor.

(4) A temporary subgroup set up by the eHealth network in accordance with Article 5(4) shall be tasked to examine any issues arising from the interoperability of national contact tracing and warning mobile applications and from the joint controllership of related processing of personal data and to facilitate coordinated instructions to the Commission as a processor. Amongst other issues, the controllers may, in the framework of the temporary subgroup, work towards a common approach on the retention of data in their national backend servers, taking into account the retention period set forth in the federation gateway.

(5) Instructions to the processor shall be sent by any of the joint controllers' contact point, in agreement with the other joint controllers in the subgroup referred to above.

(6) Only persons authorised by the designated national authorities or official bodies may access personal data of users exchanged in the federation gateway.

(7) Each designated national authority or official body shall cease to be joint controller from the date of withdrawal of its participation in the federation gateway. It shall however remain responsible for processing in the federation gateway that occurred prior to its withdrawal.

Subsection 2

Responsibilities and roles for handling requests of and informing data subjects

(1) Each controller shall provide the users of its national contact tracing and warning mobile application ('the data subjects') with information about the processing of their personal data in the federation gateway for the purposes

([1]) In particular, the interoperability specifications for cross-border transmission chains between approved apps, of 16 June 2020, available at: https://ec.europa.eu/health/ehealth/key_documents_en#anchor0

▼M1

of cross-border interoperability of the national contact tracing and warning mobile applications, in accordance with Articles 13 and 14 of the General Data Protection Regulation.

(2) Each controller shall act as the contact point for the users of its national contact tracing and warning mobile application and shall handle the requests relating to the exercise of the rights of data subjects in accordance with the General Data Protection Regulation, submitted by those users or their representatives. Each controller shall designate a specific contact point dedicated to requests received from data subjects. If a joint controller receives a request from a data subject, which does not fall under its responsibility, it shall promptly forward it to the responsible joint controller. If requested, the joint controllers shall assist each other in handling data subjects' requests and shall reply to each other without undue delay and at the latest within 15 days from receiving a request for assistance.

(3) Each controller shall make available to the data subjects the content of this Annex including the arrangements laid down in points 1 and 2.

SECTION 2

Management of security incidents, including personal data breaches

(1) The joint controllers shall assist each other in the identification and handling of any security incidents, including personal data breaches, linked to the processing in the federation gateway.

(2) In particular, the joint controllers shall notify each other of the following:

a) any potential or actual risks to the availability, confidentiality and/or integrity of the personal data undergoing processing in the federation gateway;

b) any security incidents that are linked to the processing operation in the federation gateway;

c) any personal data breach, the likely consequences of the personal data breach and the assessment of the risk to the rights and freedoms of natural persons, and any measures taken to address the personal data breach and mitigate the risk to the rights and freedoms of natural persons;

d) any breach of the technical and/or organisational safeguards of the processing operation in the federation gateway.

(3) The joint controllers shall communicate any personal data breaches with regard to the processing operation in the federation gateway to the Commission, to the competent supervisory authorities and, where required so, to data subjects, in accordance with Articles 33 and 34 of Regulation (EU) 2016/679 or following notification by the Commission.

SECTION 3

Data Protection Impact Assessment

If a controller, in order to comply with its obligations specified in Articles 35 and 36 of the General Data Protection Regulation needs information from another controller, it shall send a specific request to the functional mailbox referred to in Subsection 1(3) of Section 1. The latter shall use its best efforts to provide such information.

▼M1

ANNEX III

RESPONSIBILITIES OF THE COMMISSION AS DATA PROCESSOR FOR THE FEDERATION GATEWAY FOR CROSS-BORDER PROCESSING BETWEEN NATIONAL CONTACT TRACING AND WARNING MOBILE APPLICATIONS

The Commission shall:

(1) Set up and ensure a secure and reliable communication infrastructure that interconnects national contact tracing and warning mobile applications of the Member States participating in the federation gateway. To fulfil its obligations as data processor of the federation gateway, the Commission may engage third parties as sub-processors; the Commission shall inform the joint controllers of any intended changes concerning the addition or replacement of other sub-processors thereby giving the controllers the opportunity to jointly object to such changes as set out in Annex II, Subsection 1(4) of Section 1. The Commission shall ensure that the same data protection obligations as set out in this Decision apply to these sub-processors.

(2) Process the personal data, only based on documented instructions from the controllers, unless required to do so by Union or Member State law; in such a case, the Commission shall inform the controllers of that legal requirement before processing, unless that law prohibits submitting such information on important grounds of public interest.

(3) The processing by the Commission entails the following:

a) Authentication of national backend servers, based on national backend server certificates;

b) Reception of the data referred to in Article 7a, paragraph 3, of the Implementing Decision uploaded by national backend servers by providing an application programming interface that allows national backend servers to upload the relevant data;

c) Storage of the data in the federation gateway, upon receiving them from national backend servers;

d) Making the data available for download by national backend servers;

e) Deletion of the data when all participating backend servers have downloaded them or 14 days after their reception, whichever is earlier.

f) After the end of the provision of service, delete any remaining data unless Union or Member State law requires storage of the personal data.

The processor shall take the necessary measures to preserve the integrity of the data processed.

(4) Take all state of the art organisational, physical and logical security measures to maintain the federation gateway. To this end, the Commission shall:

▼M1

a) designate a responsible entity for the security management at the level of the federation gateway, 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 federation gateway;

c) ensure that all individuals that are granted access to the federation gateway are subject to contractual, professional or statutory obligation of confidentiality;

(5) Take all necessary security measures to avoid compromising the smooth operational functioning of the national backend servers. To this end, the Commission shall put in place specific procedures related to the connection from the backend servers to the federation gateway. This includes:

a) risk assessment procedure, to identify and estimate potential threats to the system;

b) audit and review procedure to:

i. check the correspondence between the implemented security measures and the applicable security policy;

ii. control on a regular basis the integrity of system files, security parameters and granted authorisations;

iii. monitor to detect security breaches and intrusions;

iv. implement changes to mitigate existing security weaknesses

v. allow for, 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 TFEU on the Privileges and Immunities of the European Union ([1]);

c) changing the control procedure to document and 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 their infrastructures;

d) laying down a maintenance and repair procedure to specify the rules and conditions to be respected when maintenance and/or repair of equipment should be performed;

e) laying down a security incident procedure to define the reporting and escalation scheme, inform without delay the controllers, as well as the European Data Protection Supervisor of any personal data breach and define a disciplinary process to deal with security breaches.

(6) Take state of the art physical and/or logical security measures for the facilities hosting the federation gateway equipment and for the controls of logical data and security access. To this end, the Commission shall:

([1]) Protocol (No 7) on the Privileges and Immunities of the European Union (OJ C 326, 26.10.2012, p. 266).

▼**M1**

a) enforce physical security to establish distinct security perimeters and allowing detection of breaches;

b) control access to the facilities and maintain a visitor register for tracing purposes;

c) ensure that external people granted access to the premises are escorted by duly authorised staff;

d) ensure that equipment cannot be added, replaced or removed without prior authorisation of the designated responsible bodies;

e) control access from and to the national backend servers to the federation gateway;

f) ensure that individuals who access the federation gateway are identified and authenticated;

g) review the authorisation rights related to the access to the federation gateway in case of a security breach affecting this infrastructure;

h) keep the integrity of the information transmitted through the federation gateway;

i) implement technical and organisational security measures to prevent unauthorised access to personal data;

j) implement, whenever necessary, measures to block unauthorised access to the federation gateway from the domain of the national authorities (i.e.: block a location/IP address).

(7) Take steps to protect its domain, including the severing of connections, in the event of substantial deviation from the principles and concepts for quality or security.

(8) Maintain a risk management plan related to its area of responsibility.

(9) Monitor – in real time – the performance of all the service components of its federation gateway services, produce regular statistics and keep records.

(10) Provide support for all federation gateway services in English, 24/7 via phone, mail or Web Portal and accept calls from authorised callers: the federation gateway's coordinators and their respective helpdesks, Project Officers and designated persons from the Commission.

(11) Assist the controllers by appropriate technical and organisational measures, insofar as it is possible, 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 the General Data Protection Regulation.

▼M1

(12) Support the controllers by providing information concerning the federation gateway, in order to implement the obligations pursuant to Articles 32, 35 and 36 of the General Data Protection Regulation.

(13) Ensure that data processed within the federation gateway is unintelligible to any person who is not authorised to access it.

(14) Take all relevant measures to prevent that the federation gateway's operators have unauthorised access to transmitted data.

(15) Take measures in order to facilitate the interoperability and the communication between the federation gateway's designated controllers.

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