2023/2117

13.10.2023

COMMISSION IMPLEMENTING REGULATION (EU) 2023/2117

of 12 October 2023

laying down the necessary rules and detailed requirements for the functioning and management of a repository of information pursuant to Regulation (EU) 2018/1139 of the European Parliament and of the Council

(Text with EEA relevance)

THE EUROPEAN COMMISSION,

Having regard to the Treaty on the Functioning of the European Union,

Having regard to Regulation (EU) 2018/1139 of the European Parliament and of the Council of 4 July 2018 on common rules in the field of civil aviation and establishing a European Union Aviation Safety Agency, and amending Regulations (EC) No 2111/2005, (EC) No 1008/2008, (EU) No 996/2010, (EU) No 376/2014 and Directives 2014/30/EU and 2014/53/EU of the European Parliament and of the Council, and repealing Regulations (EC) No 216/2008 and (EC) No 552/2004 of the European Parliament and of the Council and Council Regulation (EEC) No 3922/91 ([1]), and in particular Article 74(8) thereof,

Whereas:

(1) In accordance with Article 74 of Regulation (EU) 2018/1139, civil-aviation-related information is to be stored in an electronic repository of information established and managed by the European Union Aviation Safety Agency ('the Agency') necessary to ensure the effective cooperation between the Agency and the national competent authorities concerning the exercise of their tasks relating to certification, oversight and enforcement pursuant to that Regulation.

(2) It is important that the Commission and the national competent authorities are involved in the development and management of the repository by the Agency and therefore this Regulation should lay down an appropriate consultation mechanism to ensure that the Agency consults Member States and the Commission before taking decisions with regard to the repository.

(3) To ensure effective use of the repository, its structure should provide for a central database, a communication infrastructure and a necessary interface for the issue, query and access to the information stored in the repository. To ease the cooperation between the entities using the repository, there should be a single interface for a direct user queries to the repository and a single interface for the national competent authorities.

(4) The repository should facilitate the competent authorities' integration into the repository and communication with the repository through the appropriate functional specifications covering the interface, the security, the network, and application configuration information.

(5) The Agency should ensure that the repository is kept in proper conditions of working to avoid technical failures and to ensure the continuity of operation of the repository and the management of its data.

(6) The information should be transmitted to and exchanged through the repository based on commonly agreed information formats proposed by the Agency so that the exchanged information is understood in the same way by the communicating entities.

(7) Regular updates of the information stored in the repository should allow for a better exchange of information. In that regard, the Agency and the national competent authorities should develop a methodology to regularly update the information stored in the repository.

([1]) OJ L 212, 22.8.2018, p. 1.

(8) This Regulation should also establish the requirements for the classification of information so that the information stored in the repository is treated according to the privacy, confidentiality, integrity and availability parameters. A re-evaluation of this classification of information should be made whenever there is a change in the use of the data in order to ensure that the classification is up-to date.

(9) It is important to identify the interested parties that may receive information stored in the repository and to lay down detailed rules for the treatment of their requests for access. For this purpose, this Regulation should lay down the necessary conditions for the dissemination of information to the interested parties. It should also be ensured that the information received by the interested parties is managed in a confidential manner.

(10) A system of traceability of the information stored in the repository should guarantee the protection against unauthorised access to it and should enable the monitoring of the operations where information, including personal data, is processed, in order to ensure the integrity of data and information security.

(11) Staff of authorised users that need to access the repository should be authorised by their organisations following documented procedures. Staff from aeromedical centres should be authorised by their respective national competent authorities.

(12) Requirements for the protection of the relevant infrastructure and data should be developed in the framework of security management policies. In particular, measures for security management, business continuity and disaster recovery plans should be developed. The authorised users should ensure that the necessary security measures are put in place and that they cooperate in that regard.

(13) Personal data should only be processed for the purpose of ensuring effective cooperation between the Agency and the national competent authorities concerning the exercise of their tasks relating to certification, oversight and enforcement. This Regulation should set out detailed arrangements for the protection of personal data stored in the repository and exchanged through it. Such processing must comply with Regulations (EU) 2016/679 ([2]) and (EU) 2018/1725 ([3]) of the European Parliament and of the Council and clarify the responsibilities of the relevant entities designated to ensure that data protection is guaranteed.

(14) It is necessary to identify and allocate the respective responsibilities of the entities that are processing personal data in the repository, including entry and extraction of personal data from the repository. Regulation (EU) 2018/1139 provides that the Agency, in cooperation with the Commission and the National Competent Authorities establishes and manages a repository of information necessary to ensure effective cooperation between the Agency and the national competent authorities. In particular, to cooperate to ensure the security management of the repository. Therefore, they should be joint controllers for the processing of personal data for the management of the repository. Thus, it is necessary to define the responsibilities of the joint-controllers and their specific obligations towards data subjects.

(15) Each National Competent Authority, the Agency and the Commission should be the sole controller of the data processing operations performed within their own systems as authorised users. The data processing operations should be performed in accordance with Regulations (EU) 2016/679 and (EU) 2018/1725. Since data exchanged in the repository is originating from each controller, they should notify the Agency in case of any personal data breach in their system that could compromise the security, confidentiality, availability or integrity of the personal data processed in the repository.

([2]) 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).

([3]) 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).

(16) The obligation to mutually notify security breaches, including personal data breaches, should be specified to allow joint controllers identifying security incidents and data breaches as soon as possible. The necessary reporting of these breaches should be ensured by each controller accordingly.

(17) When necessary, the exercise of the rights of data subject may be restricted under certain specified conditions. These restrictions should be proportionate and limited in scope and time. The data subject should be allowed to exercise its rights to effective defence and judicial remedy.

(18) In order to ensure the safety of aviation, access to previous records, including those containing personal data, may be necessary to the competent authority. In particular, access to the medical data justifying previous unfitness periods or imposing of limitations. Therefore, and without prejudice to shorter periods provided in national law, a maximum storage period of 10 years starting from the date of expiry of the document (e.g. health certificates, medical reports, licences) including any documents necessary for the procedures referred to in Regulation (EU) 2018/1139 should ensure that this data can still be available to the authorised users.

(19) Personal data in the repository are essential information that should be kept for archiving purposes for the interest of safety of aviation and historical research purposes. After the lapse of the storage period, or of a shorter period possibly provided for in national law, personal data should be immediately deleted from the repository. Personal data may be kept for archiving purposes in public interest of aviation safety and historical research purposes outside the repository.

(20) In order to ensure the proper application of this Regulation, Member States and the affected entities should be given sufficient time to adapt their procedures to the new regulatory framework before this Regulation applies. Therefore, certain requirements of Annex I should be applicable at later dates according to their information object category and the date of issuance.

(21) The Agency has prepared a draft implementing act for the functioning and management of a repository of information pursuant to Regulation (EU) 2018/1139 and has submitted it to the Commission with Opinion No 04/2022 ([4]), in accordance with Articles 75(2), point (b), and 76(1) of Regulation (EU) 2018/1139.

(22) The European Data Protection Supervisor was consulted in accordance with Article 42(1) of Regulation (EU) 2018/1725 and delivered an opinion on 29 March 2023.

(23) The measures provided for in this Regulation are in accordance with the opinion of the Committee for the application of common safety rules in the field of civil aviation,

HAS ADOPTED THIS REGULATION:

CHAPTER I

GENERAL PROVISIONS

Article 1

Subject matter

This Regulation lays down the rules and procedures for the functioning and management of a repository of information necessary to ensure effective cooperation between the Agency and the national competent authorities concerning the exercise of their tasks relating to certification, oversight and enforcement under Regulation (EU) 2018/1139.

([4]) https://www.easa.europa.eu/document-library/opinions

Article 2

Definitions

1. For the purposes of this Regulation, the definitions of Regulations (EU) 2018/1139, (EU) 2016/679, (EU) 2018/1725, and Commission Implementing Regulations (EU) 2019/947 ([5]) and (EU) 2021/664 ([6]) shall apply.

2. The following definitions shall also apply:

(a) 'authorised users' means the Commission, the Agency, national competent authorities and any competent authority of the Member State entrusted with the investigation of civil aviation accidents and incidents as laid down in Article 74(6), first sentence, of Regulation (EU) 2018/1139;

(b) 'interface' means the point at which independent and often unrelated systems connect and act on or communicate with each other;

(c) 'authorised staff' means staff of the authorised users who have received access to the repository;

(d) 'information object category' means the type of information falling within the scope of Article 74(1) of Regulation (EU) 2018/1139 to be exchanged and accessed by the authorised users;

(e) 'information object' means an individually exchanged piece of information which shall always correspond to the information object category and be compatible with its information format;

(f) 'information format' means a pre-defined structure of the information object category consisting of a scheme of fields corresponding to detailed types of content within each information object category and vocabularies made of limited sets of permissible values associated to each field;

(g) 'interested party' means public authorities of the European Union institutions, agencies and bodies and Member States' public authorities, natural and legal persons who are subject to an information object as defined in Annex I to this Regulation and qualified entities accredited pursuant to Article 69 of Regulation (EU) 2018/1139.

CHAPTER II

ESTABLISHMENT, MANAGEMENT AND MAINTENANCE OF THE REPOSITORY

Article 3

Establishment of the repository

1. The repository shall be composed of the Storage, Exchange and User Access interfaces.

2. The Storage interface referred to in paragraph 1 shall consist of:

(a) a central database containing information referred to in Article 74(1) of Regulation (EU) 2018/1139, encompassing both the existing and new information; and

(b) a history of changes to information and its current/archived status.

3. The Exchange interface referred to in paragraph 1 shall consist of:

(a) a communication infrastructure that provides secure Application Programmable Interfaces (APIs) for the issue, change, query/read, and archive of information between the authorised users' systems and the repository; and

(b) information quality verification rules that ensure the consistency, integrity and accuracy of the information stored.

([5]) Commission Implementing Regulation (EU) 2019/947 of 24 May 2019 on the rules and procedures for the operation of unmanned aircraft (OJ L 152, 11.6.2019, p. 45).

([6]) Commission Implementing Regulation (EU) 2021/664 of 22 April 2021 on a regulatory framework for the U-space (OJ L 139, 23.4.2021, p. 161).

4. The User Access interface referred to in paragraph 1 shall provide for an online and secure query and read access to the stored information. The User Access interface shall be available only to the authorised staff.

5. The Agency shall develop the necessary documentation supporting the authorised users' integration with the repository. That documentation shall consist of:

(a) API standards and exchange mechanisms;

(b) security, network, and application configuration information required to communicate with the repository;

(c) rules specifying the valid structure and content of information exchanged with the repository.

6. The Agency shall also provide for a test environment where the authorised users can test the functionality and performance of the exchange interface between their systems and the repository.

Article 4

Management of the repository

1. The Agency shall be responsible for the operational management of the repository and shall securely store information in the repository.

2. The authorised users shall transmit to and exchange the information through the repository through the interfaces and shall ensure a secure online connection between their system(s) and the repository.

3. Before taking any decision regarding the operational management of the repository, or making it publicly available, the Agency shall consult the Commission and the national competent authorities.

4. The authorised staff of the national aeromedical examiners and aeromedical centres shall transmit and exchange the information in the repository through their national competent authorities in accordance with Article 10(4) of this Regulation.

Article 5

Maintenance of the repository

1. The Agency shall maintain the repository and ensure that it functions properly in terms of privacy, confidentiality, integrity, and availability.

2. The Agency shall systematically back up the repository and its data.

CHAPTER III

RULES ON THE INFORMATION STORED IN THE REPOSITORY

Article 6

Formats and standards of the information

1. The authorised users shall transmit, regularly update and exchange information through the repository based on commonly agreed information formats proposed by the Agency.

2. The information formats shall be standardised per information category. The authorised users shall only transmit information objects to the repository in the information format specific to that information category.

3. The list of the information objects categories is laid down in Annex I.

Article 7

Classification of information

1. The Agency, in cooperation with the Commission and the national competent authorities, shall classify the information object categories according to the following markings:

(a) privacy: non personal data, non-sensitive or sensitive personal data;

(b) confidentiality: no impact, limited, significant, catastrophic;

(c) integrity: no impact, limited, significant, catastrophic;

(d) availability: no impact, limited, significant, catastrophic.

2. The detailed definitions of the markings referred to in paragraph 1 are laid down in Annex II.

3. The Agency, in cooperation with the Commission and the national competent authorities, shall, whenever it deems necessary, re-evaluate the classification of information to ensure that it is still appropriate based on the changes in the use of information.

Article 8

Arrangements for the dissemination of information

1. The Agency may, upon request of an interested party, provide such interested party with the information contained in the repository subject to the specific conditions of use set out in this Article.

2. A request for a dissemination of information contained in the repository shall be submitted in a form and manner established by the Agency.

3. When receiving a request, the Agency shall verify that:

(a) the request is made by an interested party; and

(b) the interested party demonstrates that the requested information is strictly necessary to the interested party's own operations.

4. The Agency shall evaluate whether the request is justified and if the conditions laid down in paragraph 5 are met, it shall provide the interested party with the information requested.

5. The Agency shall provide the requested information to the interested party only under the following conditions:

(a) the interested party does not receive access to the entire content of the repository;

(b) the information is strictly necessary for the interested party's own operations;

(c) no personal data is disseminated unless such data concerns the interested party itself or if such dissemination is strictly necessary to perform the operations of the interested party.

6. The Agency shall make available to the authorised users an updated list of requests received and action taken by the Agency.

7. The interested party shall:

(a) use the information only for the purpose specified in the request form;

(b) not disclose the information received without the authorisation of the authorised users;

(c) take the necessary measures to ensure the confidentiality of the information received.

Article 9

Logging of data-processing operations

1. The Agency shall ensure that all data-processing operations are logged. The logs shall provide the following information:

(a) the purpose of the request for access to the repository;

(b) the identification of the authorised user that retrieves the data;

(c) the date and exact time of the data-processing operations;

(d) the identification of the authorised staff that carry out the search.

2. The Agency shall use the logs of the data-processing operations only for the monitoring of the lawfulness of the access to the information and for ensuring data integrity and security. The logs shall contain the data that is strictly necessary for that purpose, complying with the principle of data minimisation as laid down in Article 89 of Regulation (EU) 2016/679 and in Article 13 of Regulation (EU) 2018/1725. Logs shall be erased after the end of the monitoring procedure or at the latest after one year.

3. Upon request, the Commission and the national competent authorities shall be granted access to the logs for the purpose of assessing the lawfulness of the access to the information, monitoring the lawfulness of the data-processing operations and for ensuring data integrity and security.

Article 10

Access to the repository

1. The authorised users shall ensure that only authorised staff have access to the repository.

2. The authorised users shall ensure that its staff receives access to the information on the basis of the privacy and confidentiality markings of the information object category in accordance with Article 7.

3. The authorised users shall establish and maintain:

(a) a list of authorised staff;

(b) procedures regarding access to the repository; such procedures shall comply with the legal requirements applied to the access and processing of information laid down in Union and national law. They shall document the terms and conditions for authorised staff to access the repository.

4. The national aeromedical examiners and aeromedical centres shall ensure that only staff authorised by their national competent authority have access to the repository.

Article 11

Security management of the repository

1. The Agency shall protect the infrastructure of the repository and its information, and shall develop:

(a) a security management plan;

(b) a business continuity plan;

(c) a disaster recovery plan.

2. The Agency shall prevent the unauthorised processing of information and any unauthorised reading, copying, modification, removal or deletion of information contained in the repository or during the dissemination to or from the repository or during the transmission, in particular by means of appropriate encryption techniques.

3. The Agency shall ensure that the persons authorised to access the repository have access only to the information covered by their access authorisation, by means of individual user identities and confidential access modes only.

4. The authorised users shall manage the security of their information before and during the transmission to the repository and shall protect their infrastructure by ensuring:

(a) the establishment of interfaces between their systems and the repository;

(b) the operation and maintenance of the interfaces;

(c) that authorised staff are properly trained in information security, applicable data protection legislation and fundamental rights before they are allowed to process information stored in the repository.

5. The authorised users shall cooperate to ensure the security management of the repository.

CHAPTER IV

PERSONAL DATA PROTECTION

Article 12

Processing of personal data stored in the repository

1. Personal data stored in the repository shall only be processed to ensure cooperation between the authorised users necessary for the exercise of their tasks related to certification, oversight and enforcement. The processing shall be limited to the extent necessary for the performance of their tasks and to what is strictly necessary and proportionate to the objectives pursued.

2. The personal data shall be accessed and processed in accordance with the technical specifications of the repository.

3. The obligations of data protection by design and by default shall be taken into account both at the time of the determination of the means for processing and at the time of the processing itself.

4. The Agency shall perform regular reviews to ensure the effectiveness of all data protection safeguards implemented.

Article 13

Joint controllership of personal data processed in the repository

1. The joint controllers of the personal data stored in the repository shall be the authorised users.

2. Each joint controller shall be responsible for the fulfilment of the information classification criteria for each information object processed in the Repository.

Article 14

Allocation of responsibilities among joint controllers

1. The Agency shall be responsible for:

(a) the setting up, operation and administration of the repository;

(b) the continued management of the repository, in particular the access rights and the security and confidentiality of the personal data processed in the repository in accordance with Articles 4, 5, 9 and 12;

(c) communicating any personal data breaches within the repository to the authorised users, to the European Data Protection Supervisor and, where required, to the data subjects in accordance with Article 34 of Regulation (EU) 2018/1725;

(d) defining and implementing the technical means to enable data subjects the exercise of their rights in accordance with Regulation (EU) 2018/1725.

2. The national competent authorities and the Commission shall be responsible for:

(a) processing personal data in the repository in accordance with the Storage, Exchange and User access interfaces referred to in Article 3 and security requirements defined in paragraph 4 of Article 12;

(b) ensuring the security of any processing of personal data outside the repository when such data is processed for the purposes of or in connection to the processing through the repository;

(c) designating and communicating to the Agency the authorised staff who shall be granted access to the repository in accordance with Article 11;

(d) acting as contact point for the data subjects falling under their responsibility as sole controllers, including when they exercise their rights, using where necessary the technical means provided by the Agency in accordance with point 1(d), or through the communication channels designated in point 3;

(e) notifying the Agency of any security incident, including personal data breaches that may compromise the security, confidentiality, availability or integrity of the personal data transmitted and/or stored in the repository;

(f) notify any data breaches relating to personal data processed in the repository to the respective competent supervisory authorities and, where so required, to data subjects, in accordance with Articles 33 and 34 of Regulation (EU) 2016/679 and Article 34 of Regulation (EU) 2018/1725 as applicable.

3. Each joint controller shall designate:

(a) a point of contact with a functional mailbox for the communication amongst them;

(b) a point of contact to support data subjects in the exercise of their rights according to the applicable data protection legislation.

4. When a joint controller receives a request from a data subject who does not fall under its responsibility, it shall promptly forward the request on 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 the date on which the request for assistance was received.

5. If a controller, in order to comply with its obligations specified in Articles 33 and 34 of Regulation (EU) 2016/679 or Article 34 of Regulation (EU) 2018/1725, needs information from another controller, it shall send a specific request to the functional mailbox referred to in point 3(a). The latter shall use its best efforts to provide such information.

Article 15

Restrictions

1. The controllers may restrict the exercise of the rights of data subjects only to the extent and for as long as strictly necessary to safeguard civil aviation safety. The exercise of data subjects' rights may only be restricted in the following situations:

(a) ongoing investigations, inspections or monitoring activities referred to in Article 75(2), point (e), of Regulation (EU) 2018/1139 and performed by the Agency within the remit of its responsibilities, or by the competent authorities as provided for by national or Union law;

(b) ongoing proceedings before the Court of Justice of the European Union or any other competent court under national or international law.

2. Where the Commission and the Agency are the controllers they also may restrict the exercise of the rights of data subjects only to the extent and for as long as strictly necessary to safeguard civil aviation safety, in case of ongoing IT security investigations with a direct or indirect impact on the functioning of the repository.

3. All restrictions shall be subject to a necessity and proportionality assessment and shall be limited in scope and in time.

4. The data subject whose exercise of rights is restricted shall be informed of the grounds and the extent of the restriction.

Article 16

Storage period of personal data

1. The authorised users shall:

(a) store personal data within the repository for a maximum period of 10 years starting from the date of expiry of the document, or from the date it is no longer valid, including any documents necessary for the procedures referred to in Regulation (EU) 2018/1139 unless a different period is required by national law;

(b) delete personal data from the repository as soon as the storage period elapses.

2. The repository shall have the technical means to enable:

(a) the automated erasure of personal data upon expiry of the storage period;

(b) the automated pseudonymisation, or other technical solutions with equivalent effect, of personal data stored for archiving purposes.

Article 17

Processing for archiving and historical research purposes in the interest of safety of aviation

1. After the elapse of the storage period, the Agency may keep personal data from the repository in a separate registry for archiving and historical research purposes.

2. Such personal data shall be limited to what is strictly necessary to achieve the purposes of archiving and research in the interest of safety of aviation and complying with the principle of data minimisation as laid down in Article 89 of Regulation (EU) 2016/679 and in Article 13 of Regulation (EU) 2018/1725.

3. The Agency shall develop access protocol to the registry. Articles 4, 5 and 9 till 12 shall apply to this registry.

CHAPTER V

FINAL PROVISIONS

Article 18

Entry into force and application

1. This Regulation shall enter into force on the twentieth day following that of its publication in the *Official Journal of the European Union*.

2. Chapter I and II shall apply as of 1 April 2025.

3. The requirements concerning information objects issued after the entry into force of this Regulation shall be applicable:

(a) as of 1 January 2027 for Annex I, group A category;

(b) as of 1 January 2028 for Annex I, group B category;

(c) as of 1 January 2029 for Annex I, group C category.

4. The requirements concerning information objects which are valid and issued before the entry into force of this Regulation listed in Annex I, shall be applicable as from 1 January 2029.

This Regulation shall be binding in its entirety and directly applicable in all Member States.

Done at Brussels, 12 October 2023.

For the Commission
The President
Ursula VON DER LEYEN

ANNEX I

LIST OF INFORMATION OBJECT

Information object	Priority groups
Licences	
Pilot licence	A
Pilot licence validation	A
Air traffic controller licence	A
Aircraft maintenance licence	B
Certificates – Organisations	
ATM/ANS provider certificate	B
Aerodrome operator certificate	B
Air operator certificate (AOC)	B
Aerodrome equipment certificate	B
Certificate of airworthiness (CofA)	B
Flight simulation training devices (FSTD) qualification certificate	C
Light UAS operator certificate (LUC)	A
UAS operator certificate	C
U-space service provider (USSP) certificate	B
Common Information Service Provider certificate	B
Certificates – Personnel	
Certificate of remote pilot theoretical training	C
Examiner certificate	A
Instructor certificate	A
Language proficiency assessment center certificate	C
Certificates – Products/Equipment	
Type-certificate (TC)	B
Supplemental type-certificate (STC)	B
Restricted type certificate (RTC)	B
Type certificate data sheet	C
Noise certificate	C
Restricted noise certificate	C
Airworthiness review certificate (ARC)	C
Restricted certificate of airworthiness (RCofA)	C
Major/Minor changes approval	C
Major/Minor repair design approval	C
ATM/ANS systems and ATM/ANS constituents certificate	B
Certificates – Medical	
Aeromedical examiner certificate	A
Aeromedical centres (AeMC) certificate	A

Air traffic controller (ATCO) aeromedical examiner certificate	A
Air traffic controller (ATCO) medical certificate	A
Application form for pilot medical certificate	A
Pilot medical examination forms and supporting medical certificates	A
Pilot medical certificate	A
Declarations	
Provider of flight information services (FIS) declaration	B
Provider of apron management service declaration	B
Ground handling provider declaration	B
ATM/ANS systems and ATM/ANS constituents – declaration	B
ATM/ANS systems and ATM/ANS constituents – Statement of compliance	B
Operator declaration as provider of technical training STS	C
NCC and SPO declarations of aircraft operators	C
UAS operational declaration STS	A
Attestations and reports	
Cabin crew attestation	C
Cabin crew medical report	C
Exemptions	
Exemption (cumulative) duration above 8 months – decision	B
Exemption (cumulative) duration above 8 months – notification	B
Exemption (cumulative) duration above 8 months – recommendation	B
Exemption (cumulative) duration up to 8 months – notification	A
Exemption from holding ATM/ANS certificate as provider – decision	C
Exemption from holding ATM/ANS certificate as provider – notification	C
Exemption from holding ATM/ANS certificate as provider	C
Approvals	
Permit to fly – approval of flight conditions	A
Permit to fly	A
Maintenance Review Board (MRB) Report approval	C
Theoretical knowledge examinations (ECQB)	C
Combined Airworthiness Organisation approvals (CAOA) – Part-CAO	B
Continuing Airworthiness Management Organisation approvals (CAMOA)	B
Maintenance Organisation approvals (MOA) – Part M Subpart F EASA Form 3-MF	B
Maintenance Organisation Approvals (MOA) – Part-145	B
Maintenance Training Organisation approvals (MTOA) – Part-147	B

Letter of Agreement for production without production organisation approval	C
Production organisation approvals (POA)	B
Alternative procedure to design organisation approvals (APDOA)	C
Design organisation approvals (DOA)	B
Design or production of ATM/ANS equipment approval	B
Air traffic controller (ATCO) training organisations	B
Cabin crew training organisation (CCTO) approval	C
Training organisation (ATO) approval (Pilot)	C
Declared training organisation (DTO) for pilot	C
Ramp Inspection Training Organisation (RITO) approval	B
Decisions	
Opt-in to apply specific provisions of Basic Regulation for listed activities – decision	C
Invalidation and recognition of certificates or declarations	C
Decision to exempt from provision of Basic Regulation for Aerodromes	C
Joint responsibility for tasks relating to aircraft operators involved in commercial air transport	C
Proposal for Implementing Act/Delegated Act amendment	C
Accreditation as a Qualified Entity	C
Proposal of Individual Flight Time Specification Scheme (IFTSS)	C
Notifications of FTL schemes	C
Operator confirmation of acceptability of the updated mitigation measures and compliance of local conditions in case of cross border operations	C
Registration of UAS operator	A
Decision of a Member State on the designation of a single common information service provider	B
Measures	
Immediate measure taken in reaction to a serious safety problem (decision)	B
Immediate measure taken in reaction to a serious safety problem (recommendation)	B
Immediate measure taken in reaction to a serious safety problem (notification)	B
Conflict Zones Information Bulletins (CZIB) – Measures	B
Opt-in (Art. 2(6)) to apply specific provisions of Basic Regulation for listed activities (notification)	C
Opt-in to apply specific provisions of Basic Regulation for listed activities (recommendation)	C
Opt-out to exempt categories of aircraft from specific provisions of the Basic Regulation	C

Others	
Air operator – operations specifications	C
Third country operator's (TCO) authorisation	B
High-Risk Commercial Specialized Operations – authorisation	B
Registration of UAS certified device	A
European technical standard order authorisation (ETSOA)	C
Deviation to ETSO	C
Proposal for Implementing Act/Delegated Act amendment – notification	B
Proposal for IA/DA amendment – recommendation	B
List of Member States and Organisations having transferred responsibilities, reallocated task (in accordance with art 64 and 65) and competent authority responsible after reallocation	C
Airworthiness directives (AD), Safety directives, Safety Information Bulletins (SIB)	C
Draft recommendations for reply to ICAO State Letters	C
ICAO Standards and recommended practices (SARPs) Compliance checklist	C
Recommendations for reply to ICAO State Letters	C
Alternative Means of Compliance requests	C

ANNEX II

CLASSIFICATION OF THE INFORMATION

Detailed definitions of the markings in accordance with Article 7(2)

(a) PRIVACY is rated in accordance with the categories below:

ID	Privacy Rating Name	Privacy Rating Description
PRIV-2	Sensitive Personal Information	Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership; processing of genetic data, biometric data for the purpose of uniquely identifying a natural person; data concerning health or data concerning a natural person's sex life or sexual orientation; data concerning criminal convictions and offences
PRIV-1	Non-Sensitive Personal Information	Any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his or her physical, physiological, mental, economic, cultural or social identity and as long as they do not reveal aspects of the data subject qualifying as sensitive personal information.
PRIV-0	Non-Personal Information	Information that does not relate to a natural person or which does not lead to the identification of a natural person such as anonymised personal data.

(b) CONFIDENTIALITY is classified in accordance with the levels below:

ID	Classification Level Name	Classification Level Description
CONF-3	Catastrophic	Information whose unauthorised disclosure would have one or several of the following consequences: — Financial impact of > EUR 10 million — Significant liability/damage compensation claims by the Aviation Repository authorised users and/or interested parties — Significant competitive disadvantage for the Aviation Repository authorised users and/or interested parties — Impossibility for the Aviation Repository authorised users' to meet their objectives — Total loss of confidence by interested parties and public — Total loss of reputation — The Agency questioned as an organisation
CONF-2	Significant	Information whose unauthorised disclosure would have one or several of the following consequences: — Financial impact of EUR 1-10 million — Medium liability/damage compensation claims by the Aviation Repository authorised users and/or interested parties — Significantly damaged reputation in the specific business area, negative exposure in both specialised and general press

		— Loss of confidence by the by interested parties related to the specific business process — Breach of regulatory obligations — Breach of legal obligations — Breach of contractual requirements
CONF-1	Limited	Information whose unauthorised disclosure would have one or several of the following consequences: — Financial impact of < EUR 1 million — Minor liability/damage compensation claims by the Aviation Repository authorised users and/or interested parties — Reputation – limited negative exposure in specialised media — Loss of confidence by the internal stakeholders related to the specific business process
CONF-0	No Impact	Information whose unauthorised disclosure would cause the reputation the Aviation Repository authorised users to become inconsistent with desired image but: — No press coverage – Information is already public — No impact on interested parties — No financial impact

(c) INTEGRITY is classified in accordance with the levels below:

ID	Integrity Level Name	Classification Level Description
INTGR-3	Catastrophic	Information falling within this category is corrupted and/or compromised would have one or several of the following consequences: — Financial loss of > EUR 10 million — Significant liability/damage compensation claims by the Aviation Repository authorised users and/or interested parties — Significant competitive disadvantage for the Aviation Repository authorised users and/or interested parties Impossibility for the Aviation Repository authorised users to meet their objectives — Total loss of confidence by interested parties and public — Total loss of reputation — The Agency questioned as an organisation
INTGR-2	Significant	Information falling within this category is corrupted and/or compromised would have one or several of the following consequences: — Financial impact of EUR 1-10 million — Medium liability/damage compensation claims by the Aviation Repository authorised users and/or interested parties — Significantly damaged reputation in the specific business area, negative exposure in both specialised and general press — Loss of confidence by the by interested parties related to the specific business process — Breach of regulatory obligations — Breach of legal obligations — Breach of contractual requirements

INTGR-1	Limited	Information whose unauthorised disclosure would have one or several of the following consequences: — Financial impact of < EUR 1 million — Minor liability/damage compensation claims by the Aviation Repository authorised users and/or interested parties — Reputation – limited negative exposure in specialised media — Loss of confidence by the internal stakeholders related to the specific business process
INTGR-0	No Impact	Information whose unauthorised disclosure would cause the reputation the Aviation Repository authorised users to become inconsistent with desired image but: — No press coverage — Information is already public — No impact on interested parties — No financial impact

(d) AVAILABILITY is classified in accordance with the levels below:

ID	Availability Level Name	Classification Level Description
AVAIL-3	Catastrophic	In case of disruption, access to information needs to be re-established in a maximum period of time of 24 hours (incl. nights and week-ends)
AVAIL-2	Significant	In case of disruption, access to information needs to be re-established in a maximum period of time of 1 calendar week
AVAIL-1	Limited	In case of disruption, access to information needs to be re-established in a maximum period of time of 2 calendar weeks
AVAIL-0	No Impact	In case of disruption, access to information needs to be re-established in a maximum period of time of 1 month