EUROPEAN INSURANCE AND OCCUPATIONAL PENSIONS AUTHORITY

EIOPA-MB-14/034

10 June 2014

Decision of the Management Board concerning the Protection of Information Systems and Information

The Management Board of the European Insurance and Occupational Pensions Authority

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

Having regard to Regulation (EU) No 1094/2010 of the European Parliament and of the Council establishing the European Insurance and Occupational Pensions Authority (the "Regulation" and "EIOPA")[1], in particular Article 70(4) thereof

Having regard to Commission Decision 2001/844/EC/ECSC, Euratom of 29 November 2001 amending its internal Rules of Procedure

Whereas:

(1) Information systems play a fundamental role in the input, processing, storage and distribution of information.

(2) The security of information systems must include measures relating to technical and physical security, procedural measures and organisational measures.

(3) The European Insurance and Occupational Pensions Authority (EIOPA) has responsibility for protecting the information and the information system held.

[1] OJ L 331, 15.12.2010, p.48.

(4) It is necessary to adopt appropriate measures for applying Commission Decision 2001/844/EC/ECSC Euratom of 29 November 2001 amending its internal Rules of Procedure as required by Article 70(4) of the EIOPA Regulation.

(5) In light with the principles and objectives laid down in the Commission Decision 2001/844/EC/ECSC, it is also important to identify and implement a classification scheme for documents handled in EIOPA not defined as "EU classified information".

(6) In identifying such a scheme, EIOPA considers necessary to follow the principles laid down in Commission Decision of 16th of August 2006 C(2006) 3602.

(7) Due account should be taken of the need to protect information processed and held by EIOPA also in accordance with the obligation of professional secrecy laid down in Article 70 of the EIOPA Regulation.

(8) Any information processed in EIOPA needs to be protected to ensure that only authorised persons or those with a need to know may access them.

(9) It is important to define appropriate security measures, information systems and the information processed therein should be identified according to their level of confidentiality on the basis of the likely consequences that unauthorised disclosure might have for the interests of the Commission, the other Institutions, the Member States or other parties.

(10) These provisions are taken without prejudice to Article 15 of the TFEU and to Regulation (EC) No 1049/2001 of the European Parliament and of the Council of 30 may 2001 regarding public access to European Parliament, Council and Commission documents.

(11) These provisions are taken without prejudice to Article 16 of the TFEU and to Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data

(12) These provisions are taken without prejudice to Regulation (EEC, Euratom) No 354/83 of 1 February 1983 concerning the opening to the public of the historical archives of the European Economic Community and the European Atomic Energy Community.

Has adopted this decision:

Article 1 – Subject matter

This Decision sets out the procedures for applying Article 70(4) of the EIOPA Regulation. In particular, it provides measures for the protection of information systems and information collected, processed and stored by EIOPA.

Article 2 – Scope

1. This Decision shall be applicable to the officials, the other servants and the persons described in Article 70(1) of the EIOPA Regulation.

2. Commission Decision 2001/844/EC/ECSC applies to any EU classified information handled in EIOPA.

Article 3 – Definitions

For the purpose of this Decision the following definitions shall apply:

a) The term "information" means data in a form that allows it to be communicated, recorded or processed.

b) "EU classified information" means all information classified EU RESTRICTED, EU CONFIDENTIAL, EU SECRET or EU TOP SECRET under point 4.2a of the provisions on security annexed to Decision 2001/844/EC, ECSC, Euratom

c) The term "document" means any document as defined in Article 3(a) of Regulation (EC) No 1049/2001.

d) The term "information system" means a set of equipment, methods and procedure and, where relevant also persons, personnel, organised to perform information processing functions.

e) The term "information security" means preservation of confidentiality, integrity and availability of information.

f) The term "confidentiality" means the property that information is not made available or disclosed to unauthorized individuals, entities, or processes.

g) The term "availability" means the property of being accessible and usable upon demand by an authorized entity.

h) The term "integrity" means the property of protecting the accuracy and completeness of information.

i) The term "personal data" means personal data as defined by Article 2(a) of Regulation (EC) No 45/2001.

j) The term "processing personal data" means the processing of personal data as defined in Article 2(b) of Regulation (EC) No 45/2001.

k) The term "user" means any person to whom this Decision applies.

l) The term "handling of information" means generation, collection, storage, transmission, processing and destruction of information.

m) The term "parties" means National Competent Authorities and financial institutions.

Article 4 – Information Classification Levels

1. Information systems and the information handled shall be identified according to their level of confidentiality, integrity and availability.

2. The required levels of confidentiality, integrity and availability shall be established using a business impact assessment process, in line with the definitions given in this Decision and the security classifications laid down in Commission Decision 2001/844/EC, ECSC, Euratom.

3. For all documents not defined as "EU classified information", the levels of confidentiality referred to in point (1) are as follows:

   - "PUBLIC" shall apply to information the public disclosure of which would not be prejudicial to EIOPA. This includes information released by EIOPA for wide-spread public disclosure;

   - "EIOPA REGULAR USE" shall apply to information that is not intended for public disclosure, but the unauthorised disclosure of which would not be prejudicial to EIOPA;

   - "EIOPA RESTRICTED USE" shall apply to information the unauthorised disclosure of which would be prejudicial to EIOPA, the EU or one or more of its Member States or other parties, but not to an extent serious enough to merit EU classification as laid down in paragraph 16.1 of the provisions of Commission Decision 2001/844/EC, ECSC, Euratom;

   - "EIOPA CONFIDENTIAL USE" shall apply to information the unauthorised disclosure of which would be significantly prejudicial to EIOPA, the EU or one or more of its Member States or other parties, but not to an extent serious enough to merit EU classification as laid down in paragraph 16.1 of the provisions of the provisions of Commission Decision 2001/844/EC, ECSC, Euratom.

4. The levels of availability and integrity referred to in point 1 are as follows:

- "MODERATE" shall apply to information the loss of whose integrity or availability might threaten the internal working of EIOPA; cases would include the non-application of EIOPA's policies and procedures with limited inside impact and without any outside impact or with limited outside impact, a threat to the achievement of the objectives of a work plan or project, or the appearance of significant organisational and operational problems within EIOPA without any outside impact;

- "CRITICAL" shall apply to information the loss of whose integrity or availability might threaten the position of EIOPA with regard to the EU Institutions, Member States or other parties; cases would include damage to the image of EIOPA in the eyes of the EU Institutions, Member States, other parties or the public, a very serious prejudice to legal or natural persons, a budget overrun or a substantial financial loss with very serious adverse consequences for EIOPA's finances;

- "STRATEGIC" shall apply to information the loss of whose integrity or availability would be unacceptable to EIOPA, to the EU Institutions, to Member States to other parties because it might, for example, lead to the halting of the EIOPA's decision-making process, an adverse effect on important negotiations involving catastrophic political damage or financial losses

Article 5 – Protection of personal data

Any personal data identified in the information classified in accordance with the classification scheme provided by this Decision shall be handled in compliance with the requirements laid down in Regulation (EC) No 45/2001.

Article 6 – Implementing mechanisms

The Executive Director may develop and adopt further internal mechanisms implementing the provisions of this Decision.

Article 7 – Entry into force

This decision enters into force on 1 July 2014.

Frankfurt am Main,
[Signed]

Gabriel Bernardino
Chairperson of EIOPA

Annex 1

	EU [2011 + C(2006)3602 Decision & Implementing rules]		EIOPA 2014	
EU Classified Information	EU Top Secret	This classification shall be applied only to information and material the unauthorised disclosure of which could cause exceptionally grave prejudice to the essential interests of the EU or of one or more of its Member States	EU Top Secret	This classification shall be applied only to information and material the unauthorised disclosure of which could cause exceptionally grave prejudice to the essential interests of the EU or of one or more of its Member States
	EU Secret	This classification shall be applied only to information and material the unauthorised disclosure of which could seriously harm the essential interests of the EU or of one or more of its Member States	EU Secret	This classification shall be applied only to information and material the unauthorised disclosure of which could seriously harm the essential interests of the EU or of one or more of its Member States
	EU Confidential	This classification shall be applied to information and material the unauthorised disclosure of which could harm the essential interests of the EU or of one or more of its Member States	EU Confidential	This classification shall be applied to information and material the unauthorised disclosure of which could harm the essential interests of the EU or of one or more of its Member States
	EU Restricted	This classification shall be applied to information and material the unauthorised disclosure of which could be disadvantageous to the interests of the EU or of one or more of its Member States	EU Restricted	This classification shall be applied to information and material the unauthorised disclosure of which could be disadvantageous to the interests of the EU or of one or more of its Member States
	Limited High	For information systems or information reserved for a limited number of persons on a need to know or need to access principle and whose disclosure to unauthorised persons would cause consequential prejudice to the Commission, other institutions, Member States or other parties ,but not to an extent serious enough to merit EU classification		Information the unauthorised disclosure of which would be significantly prejudicial to EIOPA, the EU, or one or more of its member states or other parties, but not to an extent to merit EU classification as laid down in paragraph 16.1 of Commission Decision 2001/844//EC, ECSC, Euratom
	Limited Low	For information systems or information reserved for a limited number of persons on a need to know or need to access principle and whose disclosure to unauthorised persons would cause moderate prejudice to the Commission, other institutions, Member States or other parties ,but not to an extent serious enough to merit EU classification	EIOPA Restricted Use	Information the unauthorised disclosure of which would be prejudicial to EIOPA, the EU, or one or more of its member states or other parties, but not to an extent to merit EU classification as laid down in paragraph 16.1 of Commission Decision 2001/844//EC, ECSC, Euratom
			EIOPA regular Use	Information that is not intended for public disclosure, but the unauthorised disclosure of which would not be prejudicial to EIOPA
	Public	Information system or information whose public disclosure would not damage the interests of Commission, the other institutions, the Member States or other parties	Public	Information the public disclosure of which would not be prejudicial to EIOPA. This includes information released by EIOPA for wide-spread disclosure