
GDPR Contractual Obligations of AMEs as Data Processors for the UK CAA Medical Department as the Data Controller.

Document Control
Reference: GDPR AME
Contract DOC 0.5
Issue No: 1.0
Issue Date: 21 May 2018
Page: 1 of 18

1. Introduction

The GDPR includes provisions that promote accountability and governance. These complement the GDPR's transparency requirements. While the principles of accountability and transparency have previously been implicit requirements of data protection law, the GDPR's emphasis elevates their significance.

Controllers are liable for their compliance with the GDPR and must only appoint processors who can provide 'sufficient guarantees' that the requirements of the GDPR will be met and the rights of data subjects protected.

Processors must only act on the documented instructions of a controller. They will however have some direct responsibilities under the GDPR and may be subject to fines or other sanctions if they don't comply.

Whenever a controller uses a processor (a third party who processes personal data on behalf of the controller) it needs to have a written contract in place. Similarly, if a processor employs another processor it needs to have a written contract in place.

Contracts between controllers and processors ensure that they both understand their obligations, responsibilities and liabilities. These contracts help processors to comply with the GDPR, and help controllers to demonstrate their compliance with the GDPR. The use of contracts by controllers and processors may also increase data subjects' confidence in the handling of their personal data.

2. Subject Matter and duration of Processing

The AME undertakes the assessment of medical fitness for pilots and air traffic controllers (ATCO) on behalf of the UK CAA. The applicant (pilot / ATCO) will attend the AME for this assessment and the AME will undertake the medical in compliance with the EU regulations. The AME will load the medical data onto the system supplied by the UK CAA ensuring that all relevant data is accurate.

GDPR Contractual Obligations of AMEs as Data Processors for the UK CAA Medical Department as the Data Controller.

Document Control
Reference: GDPR AME
Contract DOC 0.5
Issue No: 1.0
Issue Date: 21 May 2018
Page: 2 of 18

3. Nature and purpose of the processing

The medical and personal data supplied by the applicant and processed by the AME will only be used for the assessment of medical certification in relation to the UK CAA application for pilot / ATCO medical certification.

4. Type of personal data and categories of data subject

Due to the nature of the application, personal data and sensitive medical information is collated.

5. Obligations and rights of the controller

The UK CAA, as the Data Controller, will ensure the AME is compliant with the requirements and regulations of an AME and has current AME certification to be able to access the data. The UK CAA as the Data Controller, ensures the security of the system where the AME uploads the data.

The UK CAA as the Data Controller can request to inspect the AME's premises and documentation regarding the processing of sensitive data at any time.

6. Responsibility of the Data Processor (AME)

6.1 The processor must only act on the documented instructions of the controller. If a processor determines the purpose and means of processing (rather than acting only on the instructions of the controller) then it will be considered to be a controller and will have the same liability as a controller.

6.1.1 Contractual Obligations:

- the processor must only act on the written instructions of the controller (unless required by law to act without such instructions);
- the processor must ensure that people processing the data are subject to a duty of confidence;
- the processor must take appropriate measures to ensure the security of processing;
- the processor must only engage a sub-processor with the prior consent of the data controller and a written contract;
- the processor must assist the data controller in providing subject access and allowing data subjects to exercise their rights under the GDPR;
- the processor must assist the data controller in meeting its GDPR obligations in relation to the security of processing, the notification of personal data breaches and data protection impact assessments;

Page 2 of 18



GDPR Contractual Obligations of AMEs as Data Processors for the UK CAA Medical Department as the Data Controller.

Document Control
Reference: GDPR AME
Contract DOC 0.5
Issue No: 1.0
Issue Date: 21 May 2018
Page: 3 of 18

- the processor must delete or return all personal data to the controller as requested at the end of the contract;
- the processor must submit to audits and inspections, provide the controller with whatever information it needs to ensure that they are both meeting their Article 28 obligations, and tell the controller immediately if it is asked to do something infringing the GDPR or other data protection law of the EU or a member state.

In addition to the Article 28 contractual obligations set out above, a processor has the following direct responsibilities under the GDPR. The processor must:

- co-operate with supervisory authorities (such as the ICO) in accordance with Article 31;
- ensure the security of its processing in accordance with Article 32;
- keep records of its processing activities in accordance with Article 30.2;
- notify any personal data breaches to the controller in accordance with Article 33;
- employ a data protection officer if required in accordance with Article 37; and

A processor should also be aware that:

- it may be subject to investigative and corrective powers of supervisory authorities (such as the ICO) under Article 58 of the GDPR;
- if it fails to meet its obligations, it may be subject to an administrative fine under Article 83 of the GDPR;
- if it fails to meet its GDPR obligations it may be subject to a penalty under Article 84 of the GDPR; and
- if it fails to meet its GDPR obligations it may have to pay compensation under Article 82 of the GDPR.

If a processor fails to meet any of these obligations, or acts outside or against the instructions of the controller, then it may be liable to pay damages in legal proceedings, or be subject to fines or other penalties or corrective measures.

If a processor uses a sub-processor then it will, as the original processor, remain directly liable to the controller for the performance of the sub-processor's obligations.

GDPR Contractual Obligations of AMEs as Data Processors for the UK CAA Medical Department as the Data Controller.

Document Control

Reference: GDPR AME

Contract DOC 0.5

Issue No: 1.0

Issue Date: 21 May 2018

Page: 4 of 18

7. Procedure – Reporting all incidents

- 7.1 Every incident involving personal data must be reported to the CAA Medical Data Asset Manager (DAM) via AMEsupport@caa.co.uk who can determine whether it constitutes a breach of personal data.
- 7.2 The DAM will assess whether the incident is likely to result in a risk to individuals.
- 7.3 If a risk to data subjects is likely the DAM should report this immediately to the Data Protection Manager (DPM)
- 7.4 The DPM will make a decision in conjunction with the business area (DAM and Senior Managers) on whether individuals should be contacted and whether the data breach needs to be reported to the Information Commissioner's Office.
- 7.5 If required, the DAM must ensure that following information is made available to enable the DPO (Data Protection Officer) to provide it to the ICO:
 - A description of the nature of the breach.
 - The categories of personal data affected.
 - Approximate number of data subjects affected.
 - Approximate number of personal data records affected.
 - Consequences of the breach.
 - Any measures taken to address the breach.
 - Any information relating to the data breach.
 - [Name and contact details of the DPM]

8. Procedure – Breach notification data controller to data subject

- 8.1 If the personal data breach is likely to result in high risk to the rights and freedoms of the data subject, the DAM will immediately prepare a draft notification to the data subjects that are affected (based on the standard corporate template provided by the DPM).
- 8.2 The notification to the data subject will describe the breach in clear and plain language, in addition to information specified in 7.5 above.
- 8.3 The DAM will send the notification to the DPM who will check and obtain approval of the final draft with the DPO.
- 8.4 The DPM, in conjunction with the DPO, will consult with senior managers and ExCo on the notification where necessary.

GDPR Contractual Obligations of AMEs as Data Processors for the UK CAA Medical Department as the Data Controller.

Document Control
Reference: GDPR AME
Contract DOC 0.5
Issue No: 1.0
Issue Date: 21 May 2018
Page: 5 of 18

The UK CAA Medical DAM is the owner of this document and is responsible for ensuring that this contract is agreed by the Head of Oversight and Training and the AME

AME Name:
AME Number:

AME Signature: Date:

Medical Department DAM Name:

DAM Signature: Date:

Head of Oversight & Training Name:

Head of Oversight & Training signature: Date:



GDPR Contractual Obligations of AMEs as Data Processors for the UK CAA Medical Department as the Data Controller.

Document Control
Reference: GDPR AME
Contract DOC 0.5
Issue No: 1.0
Issue Date: 21 May 2018
Page: 6 of 18

FOR INFORMATION:

ARTICLES REFERRED TO WITHIN THE CONTRACT

Article 28

Processor

1. Where processing is to be carried out on behalf of a controller, the controller shall use only processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject.
2. The processor shall not engage another processor without prior specific or general written authorisation of the controller. In the case of general written authorisation, the processor shall inform the controller of any intended changes concerning the addition or replacement of other processors, thereby giving the controller the opportunity to object to such changes.
3. Processing by a processor shall be governed by a contract or other legal act under Union or Member State law, that is binding on the processor with regard to the controller and that sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller. That contract or other legal act shall stipulate, in particular, that the processor:
 - (a) processes the personal data only on documented instructions from the controller, including with regard to transfers of personal data to a third country or an international organisation, unless required to do so by Union or Member State law to which the processor is subject; in such a case, the processor shall inform the controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest;
 - (b) ensures that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;
 - (c) takes all measures required pursuant to Article 32;
 - (d) respects the conditions referred to in paragraphs 2 and 4 for engaging another processor;
 - (e) taking into account the nature of the processing, assists the controller by appropriate technical and organisational measures, insofar as this 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;
 - (f) assists the controller in ensuring compliance with the obligations pursuant to Articles 32 to 36 taking into account the nature of processing and the information available to the processor;
 - (g) at the choice of the controller, deletes or returns all the personal data to the controller after the end of the provision of services relating to processing, and deletes existing copies unless Union or Member State law requires storage of the personal data;



GDPR Contractual Obligations of AMEs as Data Processors for the UK CAA Medical Department as the Data Controller.

Document Control
Reference: GDPR AME
Contract DOC 0.5
Issue No: 1.0
Issue Date: 21 May 2018
Page: 7 of 18

(h) makes available to the controller all information necessary to demonstrate compliance with the obligations laid down in this Article and allow for and contribute to audits, including inspections, conducted by the controller or another auditor mandated by the controller.

With regard to point (h) of the first subparagraph, the processor shall immediately inform the controller if, in its opinion, an instruction infringes this Regulation or other Union or Member State data protection provisions.

4. Where a processor engages another processor for carrying out specific processing activities on behalf of the controller, the same data protection obligations as set out in the contract or other legal act between the controller and the processor as referred to in paragraph 3 shall be imposed on that other processor by way of a contract or other legal act under Union or Member State law, in particular providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of this Regulation. Where that other processor fails to fulfil its data protection obligations, the initial processor shall remain fully liable to the controller for the performance of that other processor's obligations.

5. Adherence of a processor to an approved code of conduct as referred to in Article 40 or an approved certification mechanism as referred to in Article 42 may be used as an element by which to demonstrate sufficient guarantees as referred to in paragraphs 1 and 4 of this Article.

6. Without prejudice to an individual contract between the controller and the processor, the contract or the other legal act referred to in paragraphs 3 and 4 of this Article may be based, in whole or in part, on standard contractual clauses referred to in paragraphs 7 and 8 of this Article, including when they are part of a certification granted to the controller or processor pursuant to Articles 42 and 43.

7. The Commission may lay down standard contractual clauses for the matters referred to in paragraph 3 and 4 of this Article and in accordance with the examination procedure referred to in Article 93(2).

8. A supervisory authority may adopt standard contractual clauses for the matters referred to in paragraph 3 and 4 of this Article and in accordance with the consistency mechanism referred to in Article 63.

9. The contract or the other legal act referred to in paragraphs 3 and 4 shall be in writing, including in electronic form.

10. Without prejudice to Articles 82, 83 and 84, if a processor infringes this Regulation by determining the purposes and means of processing, the processor shall be considered to be a controller in respect of that processing.

GDPR Contractual Obligations of AMEs as Data Processors for the UK CAA Medical Department as the Data Controller.

Document Control
Reference: GDPR AME
Contract DOC 0.5
Issue No: 1.0
Issue Date: 21 May 2018
Page: 8 of 18

Article 30

Records of processing activities

1. Each controller and, where applicable, the controller's representative, shall maintain a record of processing activities under its responsibility. That record shall contain all of the following information:

(a) the name and contact details of the controller and, where applicable, the joint controller, the controller's representative and the data protection officer;

(b) the purposes of the processing;

(c) a description of the categories of data subjects and of the categories of personal data;

(d) the categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries or international organisations;

(e) where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, in the case of transfers referred to in the second subparagraph of Article 49(1), the documentation of suitable safeguards;

(f) where possible, the envisaged time limits for erasure of the different categories of data;

(g) where possible, a general description of the technical and organisational security measures referred to in Article 32(1).

2. Each processor and, where applicable, the processor's representative shall maintain a record of all categories of processing activities carried out on behalf of a controller, containing:

(a) the name and contact details of the processor or processors and of each controller on behalf of which the processor is acting, and, where applicable, of the controller's or the processor's representative, and the data protection officer;

(b) the categories of processing carried out on behalf of each controller;

(c) where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, in the case of transfers referred to in the second subparagraph of Article 49(1), the documentation of suitable safeguards;

(d) where possible, a general description of the technical and organisational security measures referred to in Article 32(1).

3. The records referred to in paragraphs 1 and 2 shall be in writing, including in electronic form.

4. The controller or the processor and, where applicable, the controller's or the processor's representative, shall make the record available to the supervisory authority on request.

GDPR Contractual Obligations of AMEs as Data Processors for the UK CAA Medical Department as the Data Controller.

Document Control

Reference: GDPR AME

Contract DOC 0.5

Issue No: 1.0

Issue Date: 21 May 2018

Page: 9 of 18

5. The obligations referred to in paragraphs 1 and 2 shall not apply to an enterprise or an organisation employing fewer than 250 persons unless the processing it carries out is likely to result in a risk to the rights and freedoms of data subjects, the processing is not occasional, or the processing includes special categories of data as referred to in Article 9(1) or personal data relating to criminal convictions and offences referred to in Article 10.

Article 31

Cooperation with the supervisory authority

The controller and the processor and, where applicable, their representatives, shall cooperate, on request, with the supervisory authority in the performance of its tasks.



GDPR Contractual Obligations of AMEs as Data Processors for the UK CAA Medical Department as the Data Controller.

Document Control
Reference: GDPR AME
Contract DOC 0.5
Issue No: 1.0
Issue Date: 21 May 2018
Page: 10 of 18

Section 2

Security of personal data

Article 32

Security of processing

1. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:

- (a) the pseudonymisation and encryption of personal data;
- (b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
- (c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
- (d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

2. In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.

3. Adherence to an approved code of conduct as referred to in Article 40 or an approved certification mechanism as referred to in Article 42 may be used as an element by which to demonstrate compliance with the requirements set out in paragraph 1 of this Article.

4. The controller and processor shall take steps to ensure that any natural person acting under the authority of the controller or the processor who has access to personal data does not process them except on instructions from the controller, unless he or she is required to do so by Union or Member State law.



GDPR Contractual Obligations of AMEs as Data Processors for the UK CAA Medical Department as the Data Controller.

Document Control
Reference: GDPR AME
Contract DOC 0.5
Issue No: 1.0
Issue Date: 21 May 2018
Page: 11 of 18

Article 33

Notification of a personal data breach to the supervisory authority

1. In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.
2. The processor shall notify the controller without undue delay after becoming aware of a personal data breach.
3. The notification referred to in paragraph 1 shall at least:
 - (a) describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;
 - (b) communicate the name and contact details of the data protection officer or other contact point where more information can be obtained;
 - (c) describe the likely consequences of the personal data breach;
 - (d) describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.
4. Where, and in so far as, it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay.
5. The controller shall document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken. That documentation shall enable the supervisory authority to verify compliance with this Article.



GDPR Contractual Obligations of AMEs as Data Processors for the UK CAA Medical Department as the Data Controller.

Document Control
Reference: GDPR AME
Contract DOC 0.5
Issue No: 1.0
Issue Date: 21 May 2018
Page: 12 of 18

Article 37

Designation of the data protection officer

1. The controller and the processor shall designate a data protection officer in any case where:

- (a) the processing is carried out by a public authority or body, except for courts acting in their judicial capacity;
- (b) the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale; or
- (c) the core activities of the controller or the processor consist of processing on a large scale of special categories of data pursuant to Article 9 and personal data relating to criminal convictions and offences referred to in Article 10. 2. A group of undertakings may appoint a single data protection officer provided that a data protection officer is easily accessible from each establishment.

3. Where the controller or the processor is a public authority or body, a single data protection officer may be designated for several such authorities or bodies, taking account of their organisational structure and size.

4. In cases other than those referred to in paragraph 1, the controller or processor or associations and other bodies representing categories of controllers or processors may or, where required by Union or Member State law shall, designate a data protection officer. The data protection officer may act for such associations and other bodies representing controllers or processors.

5. The data protection officer shall be designated on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and the ability to fulfil the tasks referred to in Article 39.

6. The data protection officer may be a staff member of the controller or processor, or fulfil the tasks on the basis of a service contract.

7. The controller or the processor shall publish the contact details of the data protection officer and communicate them to the supervisory authority.



GDPR Contractual Obligations of AMEs as Data Processors for the UK CAA Medical Department as the Data Controller.

Document Control
Reference: GDPR AME
Contract DOC 0.5
Issue No: 1.0
Issue Date: 21 May 2018
Page: 13 of 18

Article 58

Powers

1. Each supervisory authority shall have all of the following investigative powers:

- (a) to order the controller and the processor, and, where applicable, the controller's or the processor's representative to provide any information it requires for the performance of its tasks;
- (b) to carry out investigations in the form of data protection audits;
- (c) to carry out a review on certifications issued pursuant to Article 42(7);
- (d) to notify the controller or the processor of an alleged infringement of this Regulation;
- (e) to obtain, from the controller and the processor, access to all personal data and to all information necessary for the performance of its tasks;
- (f) to obtain access to any premises of the controller and the processor, including to any data processing equipment and means, in accordance with Union or Member State procedural law.

2. Each supervisory authority shall have all of the following corrective powers:

- (a) to issue warnings to a controller or processor that intended processing operations are likely to infringe provisions of this Regulation;
- (b) to issue reprimands to a controller or a processor where processing operations have infringed provisions of this Regulation;
- (c) to order the controller or the processor to comply with the data subject's requests to exercise his or her rights pursuant to this Regulation;
- (d) to order the controller or processor to bring processing operations into compliance with the provisions of this Regulation, where appropriate, in a specified manner and within a specified period;
- (e) to order the controller to communicate a personal data breach to the data subject;
- (f) to impose a temporary or definitive limitation including a ban on processing;
- (g) to order the rectification or erasure of personal data or restriction of processing pursuant to Articles 16, 17 and 18 and the notification of such actions to recipients to whom the personal data have been disclosed pursuant to Article 17(2) and Article 19;
- (h) to withdraw a certification or to order the certification body to withdraw a certification issued pursuant to Articles 42 and 43, or to order the certification body not to issue certification if the requirements for the certification are not or are no longer met;



GDPR Contractual Obligations of AMEs as Data Processors for the UK CAA Medical Department as the Data Controller.

Document Control
Reference: GDPR AME
Contract DOC 0.5
Issue No: 1.0
Issue Date: 21 May 2018
Page: 14 of 18

(i) to impose an administrative fine pursuant to Article 83, in addition to, or instead of measures referred to in this paragraph, depending on the circumstances of each individual case;

(j) to order the suspension of data flows to a recipient in a third country or to an international organisation.

3. Each supervisory authority shall have all of the following authorisation and advisory powers:

(a) to advise the controller in accordance with the prior consultation procedure referred to in Article 36;

(b) to issue, on its own initiative or on request, opinions to the national parliament, the Member State government or, in accordance with Member State law, to other institutions and bodies as well as to the public on any issue related to the protection of personal data;

(c) to authorise processing referred to in Article 36(5), if the law of the Member State requires such prior authorisation;

(d) to issue an opinion and approve draft codes of conduct pursuant to Article 40(5);

(e) to accredit certification bodies pursuant to Article 43;

(f) to issue certifications and approve criteria of certification in accordance with Article 42(5);

(g) to adopt standard data protection clauses referred to in Article 28(8) and in point (d) of Article 46(2);

(h) to authorise contractual clauses referred to in point (a) of Article 46(3);

(i) to authorise administrative arrangements referred to in point (b) of Article 46(3);

(j) to approve binding corporate rules pursuant to Article 47.

4. The exercise of the powers conferred on the supervisory authority pursuant to this Article shall be subject to appropriate safeguards, including effective judicial remedy and due process, set out in Union and Member State law in accordance with the Charter.

5. Each Member State shall provide by law that its supervisory authority shall have the power to bring infringements of this Regulation to the attention of the judicial authorities and where appropriate, to commence or engage otherwise in legal proceedings, in order to enforce the provisions of this Regulation.

6. Each Member State may provide by law that its supervisory authority shall have additional powers to those referred to in paragraphs 1, 2 and 3. The exercise of those powers shall not impair the effective operation of Chapter VII.

GDPR Contractual Obligations of AMEs as Data Processors for the UK CAA Medical Department as the Data Controller.

Document Control
Reference: GDPR AME
Contract DOC 0.5
Issue No: 1.0
Issue Date: 21 May 2018
Page: 15 of 18

Article 82

Right to compensation and liability

1. Any person who has suffered material or non-material damage as a result of an infringement of this Regulation shall have the right to receive compensation from the controller or processor for the damage suffered.
2. Any controller involved in processing shall be liable for the damage caused by processing which infringes this Regulation. A processor shall be liable for the damage caused by processing only where it has not complied with obligations of this Regulation specifically directed to processors or where it has acted outside or contrary to lawful instructions of the controller.
3. A controller or processor shall be exempt from liability under paragraph 2 if it proves that it is not in any way responsible for the event giving rise to the damage.
4. Where more than one controller or processor, or both a controller and a processor, are involved in the same processing and where they are, under paragraphs 2 and 3, responsible for any damage caused by processing, each controller or processor shall be held liable for the entire damage in order to ensure effective compensation of the data subject.
5. Where a controller or processor has, in accordance with paragraph 4, paid full compensation for the damage suffered, that controller or processor shall be entitled to claim back from the other controllers or processors involved in the same processing that part of the compensation corresponding to their part of responsibility for the damage, in accordance with the conditions set out in paragraph 2.
6. Court proceedings for exercising the right to receive compensation shall be brought before the courts competent under the law of the Member State referred to in Article 79(2).



GDPR Contractual Obligations of AMEs as Data Processors for the UK CAA Medical Department as the Data Controller.

Document Control
Reference: GDPR AME
Contract DOC 0.5
Issue No: 1.0
Issue Date: 21 May 2018
Page: 16 of 18

Article 83

General conditions for imposing administrative fines

1. Each supervisory authority shall ensure that the imposition of administrative fines pursuant to this Article in respect of infringements of this Regulation referred to in paragraphs 4, 5 and 6 shall in each individual case be effective, proportionate and dissuasive.

2. Administrative fines shall, depending on the circumstances of each individual case, be imposed in addition to, or instead of, measures referred to in points (a) to (h) and (j) of Article 58(2). When deciding whether to impose an administrative fine and deciding on the amount of the administrative fine in each individual case due regard shall be given to the following:

- (a) the nature, gravity and duration of the infringement taking into account the nature scope or purpose of the processing concerned as well as the number of data subjects affected and the level of damage suffered by them;
- (b) the intentional or negligent character of the infringement;
- (c) any action taken by the controller or processor to mitigate the damage suffered by data subjects;
- (d) the degree of responsibility of the controller or processor taking into account technical and organisational measures implemented by them pursuant to Articles 25 and 32;
- (e) any relevant previous infringements by the controller or processor;
- (f) the degree of cooperation with the supervisory authority, in order to remedy the infringement and mitigate the possible adverse effects of the infringement;
- (g) the categories of personal data affected by the infringement;
- (h) the manner in which the infringement became known to the supervisory authority, in particular whether, and if so to what extent, the controller or processor notified the infringement;
- (i) where measures referred to in Article 58(2) have previously been ordered against the controller or processor concerned with regard to the same subject-matter, compliance with those measures;
- (j) adherence to approved codes of conduct pursuant to Article 40 or approved certification mechanisms pursuant to Article 42; and
- (k) any other aggravating or mitigating factor applicable to the circumstances of the case, such as financial benefits gained, or losses avoided, directly or indirectly, from the infringement.

3. If a controller or processor intentionally or negligently, for the same or linked processing operations, infringes several provisions of this Regulation, the total amount of the administrative fine shall not exceed the amount specified for the gravest infringement.



GDPR Contractual Obligations of AMEs as Data Processors for the UK CAA Medical Department as the Data Controller.

Document Control
Reference: GDPR AME
Contract DOC 0.5
Issue No: 1.0
Issue Date: 21 May 2018
Page: 17 of 18

4. Infringements of the following provisions shall, in accordance with paragraph 2, be subject to administrative fines up to 10 000 000 EUR, or in the case of an undertaking, up to 2 % of the total worldwide annual turnover of the preceding financial year, whichever is higher:

- (a) the obligations of the controller and the processor pursuant to Articles 8, 11, 25 to 39 and 42 and 43;
- (b) the obligations of the certification body pursuant to Articles 42 and 43;
- (c) the obligations of the monitoring body pursuant to Article 41(4).

5. Infringements of the following provisions shall, in accordance with paragraph 2, be subject to administrative fines up to 20 000 000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher:

- (a) the basic principles for processing, including conditions for consent, pursuant to Articles 5, 6, 7 and 9;
- (b) the data subjects' rights pursuant to Articles 12 to 22;
- (c) the transfers of personal data to a recipient in a third country or an international organisation pursuant to Articles 44 to 49;
- (d) any obligations pursuant to Member State law adopted under Chapter IX;
- (e) non-compliance with an order or a temporary or definitive limitation on processing or the suspension of data flows by the supervisory authority pursuant to Article 58(2) or failure to provide access in violation of Article 58(1).

6. Non-compliance with an order by the supervisory authority as referred to in Article 58(2) shall, in accordance with paragraph 2 of this Article, be subject to administrative fines up to 20 000 000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher.

7. Without prejudice to the corrective powers of supervisory authorities pursuant to Article 58(2), each Member State may lay down the rules on whether and to what extent administrative fines may be imposed on public authorities and bodies established in that Member State.

8. The exercise by the supervisory authority of its powers under this Article shall be subject to appropriate procedural safeguards in accordance with Union and Member State law, including effective judicial remedy and due process.

9. Where the legal system of the Member State does not provide for administrative fines, this Article may be applied in such a manner that the fine is initiated by the competent supervisory authority and imposed by competent national courts, while ensuring that those legal remedies are effective and have an equivalent effect to the administrative fines imposed by supervisory authorities. In any event, the fines imposed shall be effective, proportionate and dissuasive. Those Member States shall notify to the Commission the provisions of their laws which they adopt pursuant to this paragraph by 25 May 2018 and, without delay, any subsequent amendment law or amendment affecting them.



GDPR Contractual Obligations of AMEs as Data Processors for the UK CAA Medical Department as the Data Controller.

Document Control

Reference: GDPR AME

Contract DOC 0.5

Issue No: 1.0

Issue Date: 21 May 2018

Page: 18 of 18

Article 84

Penalties

1. Member States shall lay down the rules on other penalties applicable to infringements of this Regulation in particular for infringements which are not subject to administrative fines pursuant to Article 83, and shall take all measures necessary to ensure that they are implemented. Such penalties shall be effective, proportionate and dissuasive.

2. Each Member State shall notify to the Commission the provisions of its law which it adopts pursuant to paragraph 1, by 25 May 2018 and, without delay, any subsequent amendment affecting them.