Changelog

VERSION	CHANGES
1.1	Changes to Clauses 7.7., 9.2., 10.4. and Appendix C.8. *(typos and updated cross-references).*
1.2	Standard completion of Appendices by Abakion
1.3	Changes to Clause C.2, 2.c
1.4	Change to Appendix B
1.5	Changes to Appendix B and Appendix C
1.6	Change in Clause 7.3 *(extended notice),* Appendix A.3 *(types of personal data),* Appendix B.1 *(updated sub-processors)* Appendix B.2 *(extended notice),* Appendix C.2 (*risk-based security level),* Appendix C.7 *(audit and inspection)* and Appendix E *(processing record removed).*

Standard Contractual Clauses

For the purposes of Article 28(3) of Regulation 2016/679 (the GDPR), with regard to the processing of personal data by the Data Processor

[NAME]
[COMPANY NO]
[ADDRESS]
[CITY AND POSTCODE]
[COUNTRY]

(the Data Controller)

and

Abakion A/S
CVR 25450272
Vibenshuset, Lyngbyvej 2
2100 Copenhagen East
Denmark

(the Data Processor)

each a ‘Party’; collectively, ‘the Parties’

HAVE AGREED on the following Standard Contractual Clauses (the Clauses) in order to meet the requirements of the GDPR and to ensure the protection of the privacy and the fundamental rights and freedoms of natural persons.

1. Table of Contents

2. Preamble

1. These Contractual Clauses (the Clauses) set out the rights and obligations of the Data Controller and the Data Processor, when processing personal data on behalf of the Data Controller.

2. The Clauses have been designed to ensure the parties' compliance with Article 28(3) of Regulation 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).

3. In the context of the provision of delivery, hosting, support, maintenance and further development of a Microsoft Dynamics solution and/or solutions on the Microsoft Power platform, the Data Processor will process personal data on behalf of the Data Controller in accordance with the Clauses.

4. The Clauses shall take priority over any similar provisions contained in other agreements between the Parties.

5. A number of appendices are attached to the Clauses and form an integral part of the Clauses.

6. Appendix A contains details about the processing of personal data, including the purpose and nature of the processing, type of personal data, categories of data subject and duration of the processing.

7. Appendix B contains the Data Controller's conditions for the Data Processor's use of sub-processors and a list of sub-processors authorised by the Data Controller.

8. Appendix C contains the Data Controller's instructions with regards to the processing of personal data by the Data Processor, a description of the minimum security measures to be implemented by the Data Processor and how audits of the Data Processor and any sub-processors are to be performed.

9. Appendix D contains provisions for other activities which are not covered by the Clauses.

10. The Clauses along with appendices shall be retained in writing, including electronically, by both Parties.

11. The Clauses shall not exempt the Data Processor from obligations to which the Data Processor is subject pursuant to the General Data Protection Regulation (the GDPR) or other legislation.

3. The rights and obligations of the Data Controller

1. The Data Controller is responsible for ensuring that the processing of personal data takes place in compliance with the GDPR (see Article 24 GDPR), the applicable EU or Member State[1] data protection provisions and the Clauses.

2. The Data Controller has the right and obligation to make decisions about the purpose(s) and means of the processing of personal data.

3. The Data Controller shall be responsible, *inter alia*, for ensuring that the processing of personal data, which the Data Processor is instructed to perform, has a legal basis.

4. The Data Processor acts according to instructions

1. The Data Processor shall process personal data only on documented instructions from the Data Controller, unless required to do so by Union or Member State law to which the processor is subject. Such instructions shall be specified in Appendices A and C. Subsequent instructions can also be given by the Data Controller throughout the duration of the processing of personal data, but such instructions shall always be documented and kept in writing, including electronically, in connection with the Clauses.

2. The Data Processor shall immediately inform the Data Controller if instructions given by the Data Controller, in the opinion of the Data Processor, contravene the GDPR or the applicable EU or Member State data protection provisions.

5. Confidentiality

1. The Data Processor shall only grant access to the personal data being processed on behalf of the Data Controller to persons under the Data Processor's authority who have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality and only on a need to know basis. The list of persons to whom access has been granted shall be kept under periodic review. On the basis of this review, such access to personal data can be withdrawn, if access is no longer necessary, and personal data shall consequently not be accessible anymore to those persons.

2. The Data Processor shall at the request of the Data Controller demonstrate that the concerned persons under the Data Processor's authority are subject to the above-mentioned obligation of confidentiality.

6. Security of processing

1. Article 32 GDPR stipulates that, 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 Data Controller and Data Processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk.

[1] References to 'Member States' made throughout the Clauses shall be understood as references to 'EEA Member States'.

The Data Controller shall evaluate the risks to the rights and freedoms of natural persons inherent in the processing and implement measures to mitigate those risks. Depending on their relevance, the measures may include the following:

a. pseudonymisation and encryption of personal data;

b. the ability to ensure 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.

Testing and assessment pursuant to (d) are, *inter alia*, included in Abakion's annual ISAE audit.

2. According to Article 32 GDPR, the Data Processor shall also – independently from the Data Controller – evaluate the risks to the rights and freedoms of natural persons inherent in the processing and implement measures to mitigate those risks. To this effect, the Data Controller shall provide the Data Processor with all information necessary to identify and evaluate such risks.

3. Furthermore, the Data Processor shall assist the Data Controller in ensuring compliance with the Data Controller's obligations pursuant to Article 32 GDPR, by *inter alia* providing the Data Controller with information concerning the technical and organisational measures already implemented by the Data Processor pursuant to Article 32 GDPR along with all other information necessary for the Data Controller to comply with the Data Controller's obligation under Article 32 GDPR.

   If subsequently – in the assessment of the Data Controller – mitigation of the identified risks requires further measures to be implemented by the Data Processor, than those already implemented by the Data Processor pursuant to Article 32 GDPR, the Data Controller shall specify these additional measures to be implemented in Appendix C.

7. Use of sub-processors

1. The Data Processor shall meet the requirements specified in Article 28(2) and (4) GDPR in order to engage another processor (a sub-processor).

2. The Data Processor shall therefore not engage another processor (sub-processor) for the fulfilment of the Clauses without the prior general written authorisation of the Data Controller.

3. The Data Processor has the Data Controller's general authorisation for the engagement of sub-processors. The Data Processor shall inform in writing the Data Controller of any intended changes concerning the addition or replacement of sub-processors at least 30 days in advance, thereby giving the Data Controller the opportunity to object to such changes prior to the engagement of the concerned sub-processor(s). The

list of sub-processors already authorised by the Data Controller can be found in Appendix B.

4. Where the Data Processor engages a sub-processor for carrying out specific processing activities on behalf of the Data Controller, the same data protection obligations as set out in the Clauses shall be imposed by the Data Processor on that sub-processor by way of a contract or other legal act under EU or Member State law, in particular providing sufficient guarantees that the sub-processor will implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of the Clauses and the GDPR.

   The Data Processor shall therefore be responsible for requiring that the sub-processor at least complies with the obligations to which the Data Processor is subject pursuant to the Clauses and the GDPR.

5. A copy of such a sub-processor agreement and any subsequent amendments shall – at the Data Controller's request – be submitted to the Data Controller, thereby giving the Data Controller the opportunity to ensure that the same data protection obligations as set out in the Clauses are imposed on the sub-processor. Clauses on business related issues that do not affect the legal data protection content of the sub-processor agreement, shall not require submission to the Data Controller.

6. The Data Processor shall agree a third-party beneficiary clause with the sub-processor where – in the event of bankruptcy of the Data Processor – the Data Controller can assume the rights of the Data Processor and assert them against sub-processors, e.g. enabling the Data Controller to instruct the sub-processor to delete or return the personal data.

7. If the sub-processor does not fulfil his data protection obligations, the Data Processor shall remain fully liable to the Data Controller as regards the fulfilment of the obligations of the sub-processor. This does not affect the rights of the data subjects under the GDPR – in particular those foreseen in Articles 79 and 82 GDPR – against the Data Controller and the Data Processor, including the sub-processor.

8. Transfer of data to third countries or international organisations

1. Any transfer of personal data to third countries or international organisations by the Data Processor shall only occur on the basis of documented instructions from the Data Controller and shall always take place in compliance with Chapter V GDPR.

2. If transfers to third countries or international organisations, which the Data Processor has not been instructed to perform by the Data Controller, are required under EU or Member State law to which the Data Processor is subject, the Data Processor shall inform the Data Controller of that legal requirement prior to processing unless that law prohibits such information on important grounds of public interest.

3. Without documented instructions from the Data Controller, the Data Processor therefore cannot within the framework of the Clauses:

   a. transfer personal data to a data controller or a data processor in a third country or in an international organisation;
   b. entrust the processing of personal data to a sub-processor in a third country;

c. process the personal data in a third country.

4. The Data Controller's instructions regarding the transfer of personal data to a third country including, if applicable, the transfer tool under Chapter V GDPR on which the transfer is based, shall be set out in Appendix C.6.

5. The Clauses shall not be confused with standard data protection clauses within the meaning of Article 46(2)(c) and (d) GDPR, and the Clauses cannot be relied upon by the Parties as a transfer tool under Chapter V GDPR.

9. Assistance to the Data Controller

1. Taking into account the nature of the processing, the Data Processor shall assist the Data Controller by appropriate technical and organisational measures, insofar as this is possible, in the fulfilment of the Data Controller's obligation to respond to requests for exercising the data subjects' rights laid down in Chapter III GDPR.

   This entails that the Data Processor shall, insofar as this is possible, assist the Data Controller in the Data Controller's compliance with:

   a. the duty to provide information when collecting personal data from the data subject;
   b. the duty to provide information when personal data have not been obtained from the data subject;
   c. the right of access by the data subject;
   d. the right to rectification;
   e. the right to erasure ('the right to be forgotten');
   f. the right to restriction of processing;
   g. notification obligation regarding rectification or erasure of personal data or restriction of processing;
   h. the right to data portability;
   i. the right to object;
   j. the right not to be subject to a decision based solely on automated processing, including profiling.

2. In addition to the Data Processor's obligation to assist the Data Controller pursuant to Clause 6.3., the Data Processor shall furthermore, taking into account the nature of the processing and the information available to the Data Processor, assist the Data Controller in ensuring compliance with:

   a. The Data Controller's obligation to without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the competent supervisory authority, the Danish Data Protection Agency (Datatilsynet), unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons;

   b. the Data Controller's obligation to without undue delay communicate the personal data breach to the data subject, when the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons;

c. the Data Controller's obligation to carry out, prior to the processing, an assessment of the impact of the envisaged processing operations on the protection of personal data (a data protection impact assessment);

d. the Data Controller's obligation to consult the competent supervisory authority, the Danish Data Protection Agency (Datatilsynet), prior to processing where a data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by the Data Controller to mitigate the risk.

3. The Parties shall define in Appendix C the appropriate technical and organisational measures by which the Data Processor is required to assist the Data Controller as well as the scope and the extent of the assistance required. This applies to the obligations foreseen in Clause 9.1. and 9.2.

10. Notification of personal data breach

1. In the event of any personal data breach, the Data Processor shall, without undue delay after having become aware of it, notify the Data Controller of the personal data breach.

2. The Data Processor's notification to the Data Controller shall, if possible, take place within 36 hours after the Data Processor has become aware of the personal data breach to enable the Data Controller to comply with the Data Controller's obligation to notify the personal data breach to the competent supervisory authority, cf. Article 33 GDPR.

3. In accordance with Clause 9(2)(a), the Data Processor shall assist the Data Controller in notifying the personal data breach to the competent supervisory authority, meaning that the Data Processor is required to assist in obtaining the information listed below which, pursuant to Article 33(3)GDPR, shall be stated in the Data Controller's notification to the competent supervisory authority:

   a. The nature of the personal data including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;

   b. the likely consequences of the personal data breach;

   c. 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. The Parties shall define in Appendix C all the elements to be provided by the Data Processor when assisting the Data Controller in the notification of a personal data breach to the competent supervisory authority.

11. Erasure and return of data

1. On termination of the provision of personal data processing services, the Data Processor shall be under obligation to return all the personal data to the Data Controller

and delete existing copies unless Union or Member State law requires storage of the personal data.

12. Audit and inspection

1. The Data Processor shall make available to the Data Controller all information necessary to demonstrate compliance with the obligations laid down in Article 28 and the Clauses and allow for and contribute to audits, including inspections, conducted by the Data Controller or another auditor mandated by the Data Controller.

2. Procedures applicable to the Data Controller's audits, including inspections, of the Data Processor and sub-processors are specified in Appendix C.7.

3. The Data Processor shall be required to provide the supervisory authorities, which pursuant to applicable legislation have access to the Data Controller's and Data Processor's facilities, or representatives acting on behalf of such supervisory authorities, with access to the Data Processor's physical facilities on presentation of appropriate identification.

13. The Parties' agreement on other terms

1. The Parties may agree other clauses concerning the provision of the personal data processing service specifying e.g. liability, as long as they do not contradict directly or indirectly the Clauses or prejudice the fundamental rights or freedoms of the data subject and the protection afforded by the GDPR. Such clauses are contained in Abakion's General Terms and Conditions as part of the overall basis of agreement.

14. Commencement and termination

1. The Clauses shall become effective on the date of both Parties' signature.

2. Both Parties shall be entitled to require the Clauses renegotiated if changes to the law or inexpediency of the Clauses should give rise to such renegotiation.

3. The Clauses shall apply for the duration of the provision of personal data processing services. For the duration of the provision of personal data processing services, the Clauses cannot be terminated unless other Clauses governing the provision of personal data processing services have been agreed between the Parties.

4. If the provision of personal data processing services is terminated, and the personal data is deleted or returned to the Data Controller pursuant to Clause 11.1. and Appendix C.4., the Clauses may be terminated by written notice by either Party.

5. Signature

On behalf of the Data Controller

Name	[NAME]
Position	[POSITION]
Telephone no.	[TELEPHONE]
E-mail address	[E-MAIL]
Signature	

On behalf of the Data Processor

Name	Kenneth Kryger Gram
Position	CEO
Telephone no.	70232317
E-mail address	kkg@abakion.com
Signature	

15. Data Controller and Data Processor contacts/contact points

1. The Parties may contact each other using the following contacts/contact points:

2. The Parties shall be under obligation continuously to inform each other of changes to contacts/contact points.

Name	[NAME]
Position	[POSITION]
Telephone no.	[TELEPHONE]
E-mail address	[E-MAIL]

Name	Kenneth Kryger Gram
Position	CEO
Telephone no.	70232317
E-mail address	Frontdesk@abakion.com

Appendix A Information about the processing

A.1. The purpose of the Data Processor's processing of personal data on behalf of the Data Controller is:

The purpose is to deliver, support, maintain and further develop the Data Controller's Microsoft Dynamics solution and/or solutions on the Microsoft Power platform.

A.2. The Data Processor's processing of personal data on behalf of the Data Controller shall mainly pertain to (the nature of the processing):

1. The Data Processor's support and maintenance of the solutions on behalf of the Data Controller. This will include processing of personal data in connection with:
    - maintenance and development, including configuration of the solution;
    - development of analyses, reports and dashboards.
2. Processing of personal data may also take place in connection with:
    - the provision of advice and guidance on data processing and the use of the solution;
    - Service and support in the utilisation and operation of the solution.

A.3. The processing includes the following types of personal data about data subjects:

The types of personal data to be processed in connection with the provision of the service will depend on the Data Controller's fields of responsibility and may include:

a) ordinary personal data such as names, addresses, telephone numbers and e-mail addresses;
b) correspondence and documents containing other personal details, e.g. from posting descriptions or posted vouchers, depending on the data controller's use of the solution;
c) national identification numbers.

Should the Data Processor's Power platform solutions - including PowerBI standard solutions - be in use, the same overview and categorisation shall be applicable, as those solutions display and utilise data from Microsoft Dynamics NAV/Business Central.

A.4. Processing includes the following categories of data subject:

The category of identified or identifiable natural persons who are data subjects covered by the Data Processing Agreement will depend on the Data Controller's fields of responsibility and may include:

a) employees,
b) clients/customers,
c) partners and counterparts.

A.5. The data processor's processing of personal data on behalf of the data controller may be performed when the Clauses commence. Processing has the following duration:

The Data Processing Agreement shall be in effect until the Parties' collaboration terminates.

Appendix B Authorised sub-processors

B.1. Approved sub-processors

On commencement of the Clauses, the Data Controller authorises the engagement of the following sub-processors:

NAME	CVR	ADDRESS	DESCRIPTION OF PROCESSING
Microsoft Ireland Ltd		One Microsoft Place, South County Business Park, Leopardstown, Dublin, D18 P521, Ireland.	Hosting of Azure servers, PowerBI, the Power platform generally, e-mail via Exchange Online and use of Microsoft 365 (Sharepoint/Teams). Dynamics 365 Customer Service is used for registering and processing support tickets. The sub-processor agreement is entitled *Microsoft Products and Services Data Protection Addendum (DPA*), and the current version at any given time can be found on Microsoft's website by searching the site or at this address: https://www.microsoft.com/licensing/docs/view/Microsoft-Products-and-Services-Data-Protection-Addendum-DPA.
Continia Software A/S	32658083	Stigborgsvej 60, 9400 Noerresundby, Denmark.	Operation of the Document Capture and Expense Management voucher solutions. Will come into play as a sub-processor only where one or more of these products are used.
Global Mediator ApS	29785465	Poppelvej 19, 3450 Alleroed, Denmark.	Provision of software engineering services in connection with Microsoft Dynamics (NAV/Business Central). Abakion uses fixed development resources from Global Mediator Aps's Ukrainian team. These skills are used in connection with product development and, by prior agreement of the customer, in connection with specific customer tasks.

NAME	CVR	ADDRESS	DESCRIPTION OF PROCESSING
Atlassian B.V.	KVK: 34311373	Singel 236 1016AB Amsterdam Netherlands	Use of Confluence and Jira for project and task management.

The Data Controller has on the commencement of the Clauses authorised the use of the abovementioned sub-processors for the processing described for that party. The Data Processor shall not be entitled – without the Data Controller's explicit written authorisation – to engage a sub-processor for a 'different' processing than the one which has been agreed upon or have another sub-processor perform the described processing.

B.2. Prior notice for the authorisation of sub-processors

The notice period for approval of any additional sub-processors is 30 working days.

Appendix C Instruction pertaining to the use of personal data

C.1. The subject of/instruction for the processing

The data processor's processing of personal data on behalf of the data controller shall be carried out by the data processor performing the following:

Support, maintenance and further development of the Microsoft Dynamics solution and Microsoft Power platform.

C.2. Security of processing

Taking into account the nature, scope, context and purpose of the processing activity, as well as the risk to the rights and freedoms of natural persons, the Data Processor shall implement an appropriate level of security.

The Data Processor shall accordingly be entitled and under obligation to make decisions about the technical and organisational security measures that are to be applied to create the necessary (and agreed) level of data security.

The data processor shall however – in any event and at a minimum – implement the following measures that have been agreed with the Data Controller:

1. The following specific requirements apply to the Data Processor's physical security:
   a) The Data Processor shall have no physical servers, but will perform processing solely via Cloud services or server accounts made available by the Data Controller.
   b) The Data Processor's premises are to be locked, and there is to be no general access to terminals at which employees work.

2. The following specific requirements apply to the Data Processor's technical security:
   a) All employee machines are to be encrypted with BitLocker.
   b) All employee machines are to undergo enforced security updates and antivirus protection.
   c) All employee passwords are set up with MFA (Multifactor Authentication).

d) Passwords, where set by the Data Processor, must be constructed in accordance with good practice and must be personal and confidential.
e) Data must be encrypted during transmission and storage.

3. The following specific requirements apply to the Data Processor's organisational security:
   a) An IT security policy is to be maintained.
   b) All employees performing data processing are to be given instructions as to what they may process, and how.
   c) All employees performing data processing are to be trained on the contents of the present Agreement.
   d) All employees of the Data Processor engaged in personal data processing under the Data Processing Agreement shall be subject to a contractual duty of confidentiality in respect of the Data Controller's information and data; data must not be disclosed to unauthorised persons or used for unauthorised purposes. The duty of confidentiality shall continue to apply after the termination of the employment relationship.

4. The following specific requirements apply to the erasure of personal data by the Data Processor:
   a) The Data Processor shall amend data only on the specific instructions of the Data Controller or in accordance with this Data Processing Agreement in connection with the termination of the Agreement.

C.3 Assistance to the data controller

The Data Processor shall insofar as this is possible – within the scope and the extent of the assistance specified below – assist the Data Controller in accordance with Clauses 9.1. and 9.2. by implementing the following technical and organisational measures:

The Data Processor shall, without undue delay following receipt, inform the Data Controller in writing of any request received by the Data Processor, direct from the data subjects or from third parties, for the exercise of data subjects' rights pursuant to Chapter III GDPR.

At the Data Controller's request, the Data Processor shall assist with the retrieval, provision and/or erasure of data as necessary for the Data Controller to comply with the regulations on the rights of data subjects pursuant to Chapter III GDPR.

The Data Processor shall assist the Data Controller to fulfil other obligations imposed on the Data Controller under the GDPR or data protection provisions of EU or Member State law.

C.4 Storage period/erasure procedures

Upon termination of the provision of personal data processing services, the Data Processor shall either delete or return the personal data in accordance with Clause 11.1., unless the Data Controller – after the signature of the Clauses – has modified the data controller's original choice. Such modification shall be documented and kept in writing, including electronically, in connection with the Clauses.

C.5 Processing location

Processing of the personal data under the Clauses cannot be performed at other locations than the following without the data controller's prior written authorisation:

The services will as a general rule be delivered from the following locations, with the inclusion of delivery from other locations in the EU as well as via hybrid work being permissible provided the stipulations of the present Agreement are observed:

Data Processor

- Abakion A/S, Vibenshuset, Lyngbyvej 2, 2100 Copenhagen East
- Abakion A/S, Skovvejen 2B, 8000 Aarhus

Data Sub-processor

- Atlassian B.V., Singel 236, 1016AB, Amsterdam, Netherlands
- Continia Software A/S, Stigborgsvej 60, 9400 Noerresundby, Denmark
- Global Mediator ApS, Poppelvej 19, 3450 Alleroed, Denmark
- Microsoft Ireland Ltd., One Microsoft Place, South Country Business Park, Leopard-stown, Dublin, D18 P521, Ireland.

C.6 Instruction on the transfer of personal data to third countries

If the Data Controller does not, in the Clauses or subsequently, provide documented instructions pertaining to the transfer of personal data to a third country, the Data Processor shall not be entitled within the framework of the Clauses to perform such transfer.

C.7 Procedures for the Data Controller's audits, including inspections, of the processing of personal data being performed by the Data Processor

The Data Processor shall arrange preparation of an auditor's report on the Data Processor's data security level and the measures taken by the Data Processor.

The auditor's report shall be prepared by a competent third party, who must be subject to the usual duty of confidentiality.

The Parties have agreed that an ISAE3000, ISAE3402 or similar audit report may be used in compliance with the Clauses. The audit report is to be prepared annually at the Data Processor's expense and may be forwarded to the Data Controller on request.

At the written request of the Data Controller, and in return for payment of a separate fee, the Data Processor may arrange preparation and submission of additional auditor's reports on matters to be agreed.

The Data Processor shall furthermore enable and contribute to audits and inspections carried out by the Data Controller or a representative thereof, to the extent necessary to verify the Data Processor's compliance with these Provisions. The Data Controller shall provide 14 calendar days' written notice of such inspections.

Any costs incurred by the Data Controller in connection with inspections shall be borne by the Data Controller itself. However, the Data Processor is obliged to allocate the resources (primarily the time) necessary for the Data Controller to carry out its inspection.

Appendix D The parties' terms of agreement on other subjects

No further terms of agreement.