Change log

VERSION	CHANGES
1.1	Amendments to Regulations 7.7., 9.2., 10.4 and Appendix C.8*(typos and updated cross-references)*
1.2	Customised for MCB customers
1.3	Clarification of B2 - notification via email
1.4	Update Appendix 2 - split by delivery platform. Raptor Services is added as a sub-processor to the MCB.Cloud platform.
1.5	Update to Appendix 2 - Heroku is adopted as UDB for Hubspot and Shopify - CloudFactory introduced as UDB for Umbraco and MCB.Cloud

Standard contractual clauses

pursuant to Article 28(3) of Regulation 2016/679 (General Data Protection Regulation) for the purposes ofprocessing of personal data by
the processor

between

Name:	Name: MCB A/S
CVR no:	CVR no.: 29150966
Address:	Address: Lægaardsvej 86B
Postcode: City	Postcode: 7500 City: Holstebro
Country:	Country: Denmark
"Data Controller"	**"Data handler"**

each of which is a "party" and together constitute the "parties"

HAVE AGREED upon the following standard contractual clauses (the Clauses) in order to comply with the General Data Protection Regulation and to ensure the protection of privacy andfundamental rights and freedoms ofindividuals

1. Content

2. Preamble

1. These Terms set out the rights and obligations of the data processor when it processes personal data on behalf of the data controller

2. These provisions are designed to ensure the Parties' compliance with Article 28(3) of 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)

3. In connection with the provision of operation, development and consultancy of web solutions and related
products, the data processor processes personal data on behalf of the data controller in accordance with theseTerms.

4. The provisions take precedence over any similar provisions in other agreements between the parties.

5. There are four appendices to these Terms and the appendices form an integral part of Terms

6. Annex A contains details on the processing of personal data, including the purpose and nature of the processing, the type of personal data, the categories of data subjects and the 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 that the data controller has authorised the use of

8. Annex C contains the data controller's instructions for the data processor's processing of personal data, a description of the security measures that the data processor must implement as a minimum and how the data processor and any sub-processors are supervised.

9. Annex D contains provisions regarding other activities not covered by the Provisions

10. The provisions and associated appendices shall be kept in writing, including electronically, by both parties

11. These Terms do not release the data processor from any obligationsimposed on theprocessor by the GDPR or any other legislation

3. Rights and obligations of the data controller

1. The controller is responsible for ensuring that personal data is processed in compliance with the General Data Protection Regulation (see Article 24 of the Regulation), data protection provisions of other EU law or[1]national law ofMember States these Cla

2. The controller has the right and obligation to make decisions about the purpose(s) and means by which personal data may be processed.

3. The data controller is responsible for, among other things, ensuring that there is a legal basis for the processing of personal data that the data processor is instructed to carry out.

4. The data processor acts on instructions

1. The processor may only process personal data on documented instructions from the controller, unless required by Union or Member State law to which the processor is subjectThis instruction shall be specified in Annexes A and C.
   Subsequent instructions may also be given by the Controller while processing personal data, but the instruction shall always be documented and kept in writing including electronically, together with these Cla

2. The processor shall immediately inform the controller ifhis or her opinionan instruction violates this Regulation or the data protection provisions of other Union or Member State law

3. The Data Processor undertakes to process the personal data only for the purpose(s), for the period and under the conditions prescribed by the Data Controller.

4. he Data Processor shall immediately inform the Data Controller ifits opinion, an instructionthis Regulation or the data protection provisions of other Union law or the national law of the Member States

5. Confidentiality

1. The data processor may only grant access to personal data processed on behalf of the data controller to persons who are subject to the data processor's powers of instruction, who have committed themselves to confidentiality or who are subject to an appropriate statutory duty of secrecy, and only to the extent necessary. The list of persons to whom access has been granted shall be reviewed on an ongoing basis. Based on this review, access to personal data may be closed if access is no longer necessary and the personal data shall no longer be accessible to these individuals.

[1] References to "Member State" in these provisions shall be construed as references to "EEA Member States".

2. The data processor shall, at the request of the data controller, be able to demonstrate that the persons concerned who are subject to the data processor's powers of instruction are subject to the above-mentioned duty of confidentiality.

6. Processing safety

1. Article 32 of the GDPR states that the controller and the processor, taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, shall implement appropriate technical and organisational measures to ensure a level of protection appropriate to those risks.

   The controller shall assess the risks to the rights and freedoms of natural persons posed by the processing and implement measures to address those risks. Depending on their relevance, this may include:

   a. Pseudonymisation and encryption of personal data.

   b. ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services.

   c. ability to restore the availability of and access to personal data in a timely manner in the event of a physical or technical incident.

   d. a procedure for regularly testing, assessing and evaluating the effectiveness of the technical and organisational measures for ensuring the security of processing.

2. According to Article 32 of the Regulation, the processor - independently of the controller - must also assess the risks to the rights of natural persons posed by the processing and implement measures to address those risks. For the purposes of this assessment, the controller shall provide the processor with the necessary information to enable the processor to identify and assess such risks.

3. In addition, the processor shall assist the controller in complying with the controller's obligation under Article 32 of the Regulation by, inter alia, making available to the controller the necessary information regarding the technical and organisational security measures already implemented by the processor pursuant to Article 32 of the Regulation and any other information necessary for the controller to comply with its obligation under Article 32 of the Regulation.

   If, in the controller's judgement, addressing the identified risks requires the implementation of additional measures to those already implemented by the processor, the controller shall specify the additional measures to be implemented in Annex C.

7. Use of sub-processors

1. The data processor must fulfil the conditions referred to in Article 28(2) and (4) of the GDPR in order to use another data processor (a sub-processor).

2. Thus, the data processor may not use a sub-processor to fulfil these Clauses without prior general written approval from the data controller.

3. The data processor has the data controller's general authorisation for the use of sub-processors. The data processor shall notify the data controller in writing of any planned changes regarding the addition or replacement of sub-processors with at least 1 month's notice, thereby giving the data controller the opportunity to object to such changes prior to the use of the sub-processor(s) in question. Longer notice periods for notification in relation to specific processing operations may be specified in Annex B.list of sub-processors already authorised by the controller can be found
in Annex B

4. Where the processor uses a sub-processor for the performance of specific processing activities on behalf of the controller, the processor shall impose on the sub-processor, by way of a contract or other legal act under Union or Member State law, the same data protection obligations as those set out in these Clauses, in particular providing appropriate guarantees that the sub-processor will implement the technical and organisational measures in such a way that the processing complies with the requirements of these Clauses and the GDPR.

   The data processor is therefore responsible for requiring the sub-processor to at least comply with the data processor's obligations under these Clauses and the GDPR.

5. Sub-processor agreement(s) and any subsequent amendments thereto shall - at the data controller's request - be sent in copy to the data controller, who thereby has the opportunity to ensure that similar data protection obligations as those arising from these Clauses are imposed on the sub-processor. Provisions on commercial terms that do not affect the data protection law content of the sub-processor agreement shall not be sent to the data controller.

6. The data processor shall include in its agreement with the sub-processor the data controller as a third party beneficiary in the event of the bankruptcy of the data processor, so that the data controller can subrogate to the data processor's rights and enforce them against sub-processors, such as enabling the data controller to instruct the sub-processor to erase or return the personal data.

7. If the sub-processor does not fulfil its data protection obligations, the processor shall remain fully liable to the controller for the fulfilment of the sub-processor's obligations. This does not affect the rights of data subjects arising from the GDPR, in particular Articles 79 and 82 of the Regulation, vis-à-vis the controller and the processor, including the sub-processor.

8. Transfer to third countries or international organisations

1. Any transfer of personal data to third countries or international organisations may only be carried out by the data processor on the basis of documented instructions from the data controller and must always be in accordance with Chapter V of the GDPR.

2. Where the transfer of personal data to third countries or international organisations, which the processor has not been instructed to carry out by the controller, is required by Union or Member State law to which the processor is subject, the processor shall inform the controller of that

legal requirement prior to processing, unless that law prohibits such notification on important grounds of public interest.

3. Thus, without documented instructions from the data controller, the data processor may not within the framework of these Clauses:

    a. transfer personal data to a controller or processor in a third country or 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 controller's instructions for the transfer of personal data to a third country, including the possible transfer basis in Chapter V of the GDPR on which the transfer is based, shall be set out in Annex C.6.

5. These Clauses shall not be confused with standard contractual clauses within the meaning of Article 46(2)(c) and (d) of the GDPR and these Clauses cannot constitute a basis for the transfer of personal data within the meaning of Chapter V of the GDPR.

9. Assistance to the controller

1. The processor shall, taking into account the nature of the processing, assist the controller as far as possible, by appropriate technical and organisational measures, in fulfilling the controller's obligation to respond to requests for the exercise of data subjects' rights as laid down in Chapter III of the GDPR.

    This means that the data processor shall, as far as possible, assist the data controller in connection with the data controller's obligation to ensure compliance:

    a. the obligation to provide information when collecting personal data from the data subject
    b. the obligation to provide information if personal data has not been collected from the data subject
    c. right of access
    d. the right to rectification
    e. the right to erasure ("right to be forgotten")
    f. the right to restriction of processing
    g. the notification obligation in connection with 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, taking into account the nature of the processing and the information available to the data processor, further assist the data controller by

a. the controller's obligation to report a personal data breach to the competent supervisory authority, the Danish Data Protection Agency, without undue delay and, if possible, no later than 72 hours after becoming aware of it, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons

b. the controller's obligation to notify the data subject without undue delay of a personal data breach where the breach is likely to result in a high risk to the rights and freedoms of natural persons

c. the controller's obligation to carry out a pre-processing analysis of the impact of the envisaged processing activities on the protection of personal data (an impact assessment)

d. the controller's obligation to consult the competent supervisory authority, the Data Protection Authority, prior to processing where a data protection impact assessment shows that the processing will lead to a high risk in the absence of measures taken by the controller to mitigate the risk.

3. The parties shall specify in Annex C the necessary technical and organisational measures with which the data processor shall assist the data controller and to what extent and scope. This applies to the obligations arising from Clauses 9.1 and 9.2.

10. Personal data breach notification

1. The data processor shall notify the data controller without undue delay after becoming aware that a personal data breach has occurred.

2. The data processor's notification to the data controller shall, if possible, be made no later than 60 hours after it has become aware of the breach, so that the data controller can fulfil its obligation to notify the personal data breach to the competent supervisory authority, cf. Article 33 of the GDPR.

3. In accordance with Clause 9.2.a, the processor shall assist the controller in notifying the breach to the competent supervisory authority. This means that the processor shall assist in providing the following information, which according to Article 33(3) must be included in the controller's notification of the breach to the competent supervisory authority:

    a. the nature of the personal data breach, including, where possible, the categories and approximate number of data subjects affected and the categories and approximate number of personal data records affected

    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 applicable, measures to mitigate its possible adverse effects.

4. The parties shall specify in Annex C the information that the processor shall provide in connection with its assistance to the controller in its obligation to notify personal data breaches to the competent supervisory authority.

11. Deletion and return of data

1. Upon termination of the personal data processing services, the processor shall be obliged to either erase all personal data that have been processed on behalf of the controller and confirm to the controller that the data have been erased. Or, alternatively, to return all personal data and delete existing copies, unless Union or Member State law provides for the retention of the personal data.

12. Audit, including inspection

1. The Processor shall make available to the Controller all information necessary to demonstrate compliance with Article 28 of the GDPR and these Clauses and shall allow for and contribute to audits, including inspections, carried out by the Controller or another auditor authorised by the Controller.

2. The procedures for the controller's audits, including inspections, with the data processor and sub-processors are detailed in Appendices C.7. and C.8.

3. The data processor is obliged to grant access to the data processor's physical facilities to supervisory authorities that have access to the data controller's or data processor's facilities under applicable law, or representatives acting on behalf of the supervisory authority, against proper identification.

13. The parties' agreement on other matters

1. The parties may agree on other provisions regarding the service relating to the processing of personal data, such as liability, as long as these other provisions do not directly or indirectly contravene the Clauses or impair the fundamental rights and freedoms of the data subject arising from the GDPR.

14. Entry into force and termination

1. The provisions shall enter into force on the date of signature by both parties.

2. Both parties may demand renegotiation of the Terms and Conditions if changes in the law or inappropriateness of the Terms and Conditions give rise to this.

3. The Terms are valid for the duration of the Personal Data Processing Service. During this period, the Terms cannot be cancelled, unless other provisions governing the provision of the Personal Data Processing Service are agreed between the parties.

4. If the provision of the Personal Data Processing Services ceases and the Personal Data has been deleted or returned to the Controller in accordance with Clause 11.1 and Appendix C.4, the Clauses may be terminated by either party upon written notice.

5. Your signature
On behalf of the data controller

	On behalf of the data processor
Name:	
Position:	Name: Bo Hedegaard Rasmussen
Telephone:	Position: Director
Email:	Phone: 4082 5863
	E-mail: bhk@mcb.dk
_____	
Your signature	Your signature

15. Contact persons at the data controller and data processor

1. The parties can contact each other via the contact persons below.

2. The parties are obliged to regularly inform each other of changes regarding contact persons.

Name:	
Position:	
	Name: Jesper Navntoft Pedersen
Telephone:	
	Position: Head of department
Email:	
	Phone: 2222 0432
	E-mail: jnp@mcb.dk

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

The Data Controller receives assistance for the operation, hosting and development of web-related services.

A.2. The processing of personal data by the data processor on behalf of the data controller primarily concerns (nature of the processing)

The data processor will have access to personal data in systems to which access has been granted by the data controller

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

A.4. The processing involves the following categories of data subjects

Private individuals

A.5 The data processor's processing of personal data on behalf of the data controller may commence after the entry into force of these Provisions. The processing has the following duration

The processing takes place as long as the Data Controller has cooperation with the Data Processor, i.e. until the Data Controller cancels the agreement with the Data Processor.

Appendix B: Sub-processors

B.1. Authorised sub-processors

Upon entry into force of the Clauses, the Controller has authorised the use of the following sub-processors

MCB.Cloud and Education

NAME	CVR	ADDRESS	DESCRIPTION OF TREATMENT
Lynero ApS/ DLX A/S	32085571/ 28692986	Hammerhusvej 16C 7400 Herning +45 7020 1272 kontakt@lynero.dk	For MCB.Cloud customers Sub-processor provides and operates the physical infrastructure for the virtual hosting environment where the Data Controller's IT system is run, including servers, network, storage system, firewall, internet connection, power supplies, fire extinguishing equipment and cooling. Data backup is also provided.
John Nielsen		Calle Sierra Guadalupe 14 30163 Esparragal, Murcia. Spain	Assists with development and server operations.
MCB LT		Laisvės g. 14, 89223 Mažeikiai, Lithuania	MCB LT assists with development
Raptor	DK35055975	Åboulevarden 37, 4. 8000 Aarhus C	Product profiling and recommendation. For MCB.Cloud customers who use personalisation in the platform, it is understood that MCB uses Raptor as a sub-processor for this service.
CloudFactory	DK35393692	Vestergade 4 6800 Varde	Manage connection to MS Azure. Services are used for generative AI of articles and products.

Magento, Wordpress, WooCommerce (PHP)

NAME	CVR	ADDRESS	DESCRIPTION OF TREATMENT
MCB Vietnam		5th floor, No. 58, Alley 221 Ton Duc Thang Str., Dong Da Hanoi, Vietnam contact@mcb.vn	MCB Vietnam assists with development according to SCC - see item C6.
Powerhosting ApS	33055048	Dalgasgade 11 7400 Herning	For Magento platform customers Sub-processor provides and operates the physical infrastructure for the virtual hosting environment where the Data Controller's IT system is run, including servers, network, storage system, firewall, internet connection, power supplies, fire extinguishing equipment and cooling. Data backup is also provided.

Umbraco

NAME	CVR	ADDRESS	DESCRIPTION OF TREATMENT
MCB LT		Laisvės g. 14, 89223 Mažeikiai, Lithuania	MCB LT assists with development
CloudFactory	35393692	Vestergade 4 6800 Varde	Manage connection to MS Azure. Web solution hosting

Shopify

NAME	CVR	ADDRESS	DESCRIPTION OF TREATMENT
MCB Vietnam		5th floor, No. 58, Alley 221 Ton Duc Thang Str., Dong Da Hanoi, Vietnam contact@mcb.vn	MCB Vietnam assists with development according to SCC - see item C6.
Heroku		Salesforce UK Limited, Floor 26 Salesforce Tower, 110 Bishopsgate, London, EC2N 4AY, United Kingdom,	Cloud hosting of services and apps for shopify customers.

Hubspot

NAME	CVR	ADDRESS	DESCRIPTION OF TREATMENT
Heroku		Salesforce UK Limited, Floor 26 Salesforce Tower, 110 Bishopsgate, London, EC2N 4AY, United Kingdom,	Cloud hosting of services and apps for shopify customers.

Digital Marketing
It is the customer's responsibility to have data processing agreements with the 3rd party products and services used for marketing.

Upon the entry into force of the Clauses, the data controller has authorised the use of the above-mentioned sub-processors for the described processing activity. The data processor may not - without the data controller's written authorisation - use a sub-processor for a processing activity other than that described and agreed or use another sub-processor for this processing activity.

B.2. Notification for authorisation of sub-processors

1. Commissioning of a new sub-processor
   MCB must inform the data controllers when entering into an agreement with a new sub-processor who will have access to the data processors' system and data.
   Notification is made to the e-mail address registered with MCB's accounting department as the invoice recipient.

2. Change to data processor:
   MCB's sub-processors are generally authorised, and changes to sub-processors that do not directly affect contracts or the agreed delivery areas may be made without notification to the data controller.

Appendix C: Instructions for processing personal data

C.1 Subject matter/instruction of the treatment

The data processor's processing of personal data on behalf of the data controller takes place by the data processor performing the following:

Data Processor advises on systems containing personal data, exchanges data between systems containing personal data, stores (hosting and backup) data containing personal data, develops systems containing personal data.

C.2 Security of processing

The level of security should reflect this:

The processing includes sensitive personal data and thus special categories of personal data, cf. Article 9 of the General Data Protection Regulation. This means that a high level of security must be established around the processing.

The data processor is then entitled and obliged to make decisions on which technical and organisational security measures to implement in order to establish the necessary (and agreed) security level.

However, the Processor shall - in any event and as a minimum - implement the following measures agreed with the Controller:

1. **Authorisation and access control**
   Physical access control to the Processor's premises.

2. **Staff with access to personal data**
   Only selected employees may have access to the personal data that the Data Processor processes on behalf of the Data Controller. Employees with access to personal data must be authorised via a described approval procedure and access must be via Active Directory. The Data Processor shall at least once a year conduct an annual review to ensure that only authorised persons at the Data Processor continue to have access to the personal data.

3. **Control of rejected access attempts**
   The Data Processor shall continuously monitor rejected access attempts to the Data Controller's personal data placed in the Data Processor's custody. At the 5th rejected access attempt, the account must be locked.

4. **Confidentiality**
   Employees with access to the Controller's personal data must have signed a confidentiality agreement.

5. **Logging**
   The data processor must keep logging in accordance with the requirements that previously followed from the Security Executive Order, i.e. the logging must at least contain information about time, user, types of use and indication of the person the information used concerned or the search criterion used (Section 19(1) of the Security Executive Order).

6. **Home workspaces**

Home workplaces may be used by the Data Processor provided that these home workplaces fulfil the requirements of the Danish Data Protection Agency applicable from time to time and that the Data Processor has ensured the same level of security at the home workplaces as follows from this agreement. Access to personal data in the event of a physical or technical incident The Data Processor shall at all times ensure secure access to the personal data that the Data Processor processes on behalf of the Data Controller. This in the form of a separate backup located at a different physical location than the location where the normal personal data is processed. The data must be able to be restored and made available again within 24 hours after such an incident may have occurred. This backup must be stored under appropriate technical and organisational security measures that follow from the GDPR and the conditions that follow from this Data Processing Agreement.

7. **Transfer/transmission of personal data**
   The transmission of personal data must be carried out under appropriate security measures. This means that the personal data must be protected during the transmission itself. This could be in the form of encryption, setting up firewalls or similar. Requirements for storage of personal data The personal data must be stored within the EU and under appropriate security measures. Appropriate security measures could for example be the setting up of firewalls, encryption or similar.

C.3 Assistance to the controller

The data processor shall, as far as possible - within the scope and extent set out 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, where deemed necessary, inform data subjects of their rights. This applies both in situations where the data is collected directly from the data subject and in situations where the

The Data Controller shall transfer the data directly to the Data Processor for the purpose of processing the data. The Data Processor shall set up an internal procedure to ensure that the data subjects' rights are handled correctly and in a timely manner. This also applies to the further information of the Data Controller.

C.4 Retention period/deletion routine

Personal data is stored for as long as necessary, which is normally the period of the agreement with the Data Controller, after which the personal data is deleted by the Data Processor.

Data is deleted 90 days after the end of trading and can be backed up for a further 90 days.

C.5 Location of treatment

Processing of the personal data covered by the Clauses may not, without the data controller's prior written authorisation, take place at other locations at MCB's address Leggaarvej 86, 7500 Holstebro, Denmark, or at the sub-processors listed in Appendix B1.

C.6 Instructions for the transfer of personal data to third countries

The Data Controller has given general consent for the Data Processor and its subcontractors to transfer personal data to third countries to the extent that the European Commission has determined that the third country, territory in a third country, a sector in a third country or an international organisation located in a third country is secure and thus has a level of protection essentially equivalent to the level of protection applicable in the EU.Furthermore, it means that the Data Controller has also approved that the Data Processor or its subcontractors may transfer personal data to organisations in third countries that are under the EU Standard Contractual
Clauses (SCC)

If the Data Controller has not specified in this section or by a subsequent written notice an instruction or authorisation regarding the transfer of personal data to a third country, the Data Processor may not carry out such a transfer within the framework of the Data Processing Agreement.

There are technical measures in place to prevent access to sensitive personal data outside the EU.

C.7 Procedures for audits, including inspections, by the controller of the processing of personal data entrusted to the processor

The parties agree that the following types of ISAE - 3401/2 may be used in accordance with these Provisions:

The data controller or a representative of the data controller may, upon request, carry out a physical inspection of the premises from which the data processor carries out the processing of personal data, including physical premises and systems used for or in connection with the processing,
for the purpose of determining the data processor's compliance with the GDPR, data protection provisions in other EU or Member State law and these Clauses.

In addition to the planned supervision, the controller may carry out an inspection at the data processor's premises when the controller deems it necessary.

Any costs incurred by the data controller in connection with a physical inspection shall be borne by the data controller on a T&M basis. However, the data processor is obliged to allocate the resources (mainly the time) necessary for the data controller to carry out its inspection.

C.8 Procedures for audits, including inspections, of the processing of personal data entrusted to sub-processors.

The Data Processor or a representative of the Data Processor may once a year conduct a physical inspection of the sub-processor's compliance with this Data Processing Agreement.

In addition to this annual supervision, the sub-processor may be supervised when, in the reasonable judgement of the Data Processor (or the Data Controller), a need arises.

Documentation of the inspections carried out shall be sent to the Data Controller for information as soon as possible.

The Data Controller may - if deemed necessary - choose to initiate and participate in a physical inspection of the sub-processor. However, this may only be relevant if the Data Controller documents that the Data Processor's supervision of the sub-processor has not provided the Data Controller with sufficient assurance that the processing at the sub-processor is in accordance with this Data Processing Agreement.

Any expenses incurred by the Data Processor and Sub-Processors in connection with the organisation of a physical supervision/inspection at the Sub-Processor's premises shall be of no concern to the Data Controller.

Appendix D: The parties' regulation of other matters