DATA PROTECTION DUE DILIGENCE ON SELLER

Version 1.0

1. Data Catalogue/Data Maps

Provide a copy of the Company's processing activities in relation to the business and any data catalogue's or maps detailing the processing operations.

Provide details of the Company's systems, policies and procedures for keeping these up to date.

Provide a copy of any register of processing activities maintained for the purposes of compliance with data protection laws.

2. Lawful Basis

For the purposes of any personal data transferred by the Company as part of the transaction specify how the Company intends to undertake such transfer in compliance with Data Protection laws.

Provide a description of all processing undertaken by the Business describing the role of the Company in relation to the processing activity (ie, as controller, processor, sub processor, joint controller) and in the case where Company is a controller, for any processing activity, the personal data processed and the lawful basis for the processing providing further details as described below where applicable:

2.1. Contract

If processing is based on a contract then provide a copy of the contract

2.2. Consent

If processing is based on consent then provide a copy of the consent obtained

2.3. Legitimate Interest

If processing is based on Legitimate Interest then provide a description of the legitimate interest and a copy of the legitimate interest assessment undertaken

2.4. Legal Obligation

If processing is based on a Legal Obligation identify the legal obligation by providing the full name of the relevant law and the relevant provision providing for the processing as part of that law.

2.5. Vital Interest

If processing is based on vital interest, identify the vital interest and justify why no other legal basis would be appropriate

2.6. Public Interest or Official Authority

If processing is based on public interest or official authority identify the public interest/identify the official authority

2.7. Other Lawful Basis

If other legal basis set out in local law are used but not set out here then identify the lawful basis and the relevant provision under local law.

If processing personal data relating to criminal convictions identify the lawful basis

If processing special categories of personal data, identify the lawful basis

3. Privacy Notices and Statements

Provide a copy of:

(i) Website privacy notice

(ii) Privacy statement

(iii) Employee privacy notice

4. Assessments

Provide a copy of all data protection assessments undertaken by the Company relating to the business including:

(i) Legitimate Interest Assessments

(ii) Data Protection Impact Assessments

5. Policies and Procedures

Provide a copy of all data protection related policies and procedures including (as applicable):

(i) The Data Protection Policy

(ii) The (Personal) Data Retention Policy

(iii) The Breach Management Policy

(iv) The Data Subject Access Request Policy

(v) CCTV Policy

Provide details of, and copies of any documents relating to, the Company's policies, procedures, systems and processes for:

(i) ensuring its compliance with data protection law in relation to the business;

(ii) dealing with data subject notices or requests (such as requests to access their personal data, prevent the use of their personal data for direct marketing, require the erasure or rectification of their personal data, or exercising their rights to be forgotten, data portability or to object to the processing of their personal data); and

(iii) conducting data protection impact assessments

6. Technical and Organisational Measures

Provide a copy of Technical and Organisational Measures including all policies, procedures, systems and processes to:

(i) safeguard and back up data (including personal data)

(ii) respond to a data security breach

(iii) test security measures. Provide a copy of any tests undertaken by Company or a third party

(iv) ensure confidentiality of processing by persons carrying out the processing (employees and 3rd parties)

(v) ensure data protection policies and procedures are followed

(vi) ensure policies and procedures are regularly reviewed and updated

(vii) manage data processing outsourcing arrangements including evaluation and audit of suppliers

(viii) ensure employees are provided with appropriate training and awareness of data protection activities

(ix) implement privacy by design

(x) maintain logs of data processing activities

7. Breach Management

Provide a copy of the following in respect of the last six (6) years:

(i) all policies and procedures in place for the purposes of breach management
(ii) a log of all breaches investigated by the Company
(iii) a copy of all breaches reported to any supervisory authority
(iv) a copy of breach notifications provided to the data subject
(v) all documents of steps taken to mitigate the effect of any breaches

8. Supplier Due Diligence

Provide evidence of all due diligence undertaken in relation to third party processors including:

(i) internal supplier due diligence checklists
(ii) due diligence forms completed by the processor
(iii) supplier audits undertaken by the Company or any third party at the request of the Company and related reports

Provide copies of all relevant supplier contracts including a copy of the Data Processing Agreement and agreed technical and organisational measures with the supplier.

9. International Transfers

Provide details of any personal data transferred outside the EEA by the Seller in relation to the business and the transfer mechanism used in respect of such transfer. Provide evidence of the transfer mechanism.

Provide details of any extra jurisdictional transfers undertaken by processors used by the Company and a copy of the relevant agreement ensuring such transfers are compliant.

10. Staff

(i) Provide details of and evidence that staff have been provided with an appropriate level of training to meet the requirements of data protection laws

(ii) Provide a copy of confidentiality undertakings signed by employees

(iii) Provide details of, and copies of all documents relating to, any data protection officer appointed by the Company in relation to the business in accordance with data protection laws or otherwise, or any privacy manager or similar officer appointed to manage the Seller's privacy governance structure.

(iv) Provide details of any privacy team appointed in the Company and any project plan for GDPR compliance in place

11. Audits

Provide a copy of any audit of data protection processing activities undertaken in the past six years:

(i) Internally

(ii) by any third party

(iii) by any supervisory authority

12. Certifications

Provide information on any relevant certifications (ISO, BSI or other).