Data Processing Agreement

Definitions
In this Agreement:

Applicable Law	means as applicable and binding on the Customer, the Company, the Licensed Programs and/or the Services: (a) any law, statute, regulation, by-law or subordinate legislation in force from time to time to which a party is subject and/or in any jurisdiction that the Services are provided to or in respect of; (b) the common law and laws of equity as applicable to the parties from time to time; (c) any binding court order, judgment or decree; or (d) any applicable direction, policy, rule or order that is binding on a party and that is made or given by any regulatory body having jurisdiction over a party or any of that party's assets, resources or business;
Appropriate Safeguards	means such legally enforceable mechanism(s) for transfers of Personal Data as may be permitted under Data Protection Laws from time to time;
Data Controller	has the meaning given to that term (or to the term 'controller') in Data Protection Laws;
Data Processor	has the meaning given to that term (or to the term 'processor') in Data Protection Laws;
Data Subject	has the meaning given to that term in Data Protection Laws;
Data Subject Request	means a request made by a Data Subject to exercise any rights of Data Subjects under Data Protection Laws;
Data Protection Laws	means as applicable and binding on the Customer, the Company, the Licensed Programs and/or the Services: (a) in the United Kingdom: (i) the Data Protection Act 1998 and any laws or regulations implementing Directive 95/46/EC (Data Protection Directive); and/or (ii) the GDPR, and/or any corresponding or equivalent national laws or regulations; (b) in member states of the European Union: the Data Protection Directive or the GDPR, once applicable, and all relevant member state laws or regulations giving effect to or corresponding with any of them; and (c) any Applicable Laws replacing, amending, extending, re-enacting or consolidating any of the above Data Protection Laws from time to time;
Data Protection Losses	means all liabilities, including all: (a) costs (including legal costs), claims, demands, actions, settlements, interest, charges, procedures, expenses, losses and damages (including relating to material or non-material damage); and (b) to the extent permitted by Applicable Law:

	(i) administrative fines, penalties, sanctions, liabilities or other remedies imposed by a Supervisory Authority; (ii) compensation which is ordered by a Supervisory Authority to be paid to a Data Subject; and (iii) the reasonable costs of compliance with investigations by a Supervisory Authority;
GDPR	means the General Data Protection Regulation (EU) 2016/679;
GDPR Date	means from when the GDPR applies on 25 May 2018;
international organisation	means an organisation and its subordinate bodies governed by public international law, or any other body which is set up by, or on the basis of, an agreement between two or more countries;
International Recipient	has the meaning given to that term in clause 6.1;
Personal Data	has the meaning given to that term in Data Protection Laws;
Personal Data Breach	means any breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, any Protected Data;
processing	has the meanings given to that term in Data Protection Laws (and related terms such as **process** have corresponding meanings);
Processing Instructions	has the meaning given to that term in clause 2.1.1;
Protected Data	means Personal Data received from or on behalf of the Customer in connection with the performance of the Company's obligations under this Agreement;
Sub-Processor	means another Data Processor engaged by the Company for carrying out processing activities in respect of the Protected Data on behalf of the Customer;
Supervisory Authority	means any local, national or multinational agency, department, official, parliament, public or statutory person or any government or professional body, regulatory or supervisory authority, board or other body responsible for administering Data Protection Laws;

Specific interpretive provision(s)
In clauses 1 to 11 (inclusive):

1 references to any Applicable Laws (including to the Data Protection Laws and each of them) and to terms defined in such Applicable Laws shall be replaced with or incorporate (as the case may be) references to any Applicable Laws replacing, amending, extending, re-enacting or consolidating such Applicable Law (including the GDPR and any new Data Protection Laws from time to time) and the equivalent terms defined in such Applicable Laws, once in force and applicable; and

2 a reference to a law includes all subordinate legislation made under that law;

Data processing provisions

1 Data Processor and Data Controller

1.1 The parties agree that, for the Protected Data, the Customer shall be the Data Controller and the Company shall be the Data Processor.

1.2 The Company shall process Protected Data in compliance with:

1.2.1 the obligations of Data Processors under Data Protection Laws in respect of the performance of its obligations under this Agreement; and

1.2.2 the terms of this Agreement.

1.3 The Customer shall comply with:

1.3.1 all Data Protection Laws in connection with the processing of Protected Data, the Services and the exercise and performance of its respective rights and obligations under this Agreement, including maintaining all relevant regulatory registrations and notifications as required under Data Protection Laws; and

1.3.2 the terms of this Agreement.

1.4 The Customer warrants, represents and undertakes, that:

1.4.1 all data sourced by the Customer for use in connection with the Services shall comply in all respects, including in terms of its collection, storage and processing (which shall include the Customer providing all of the required fair processing information to, and obtaining all necessary consents from, Data Subjects), with Data Protection Laws;

1.4.2 all instructions given by it to the Company in respect of Personal Data shall at all times be in accordance with Data Protection Laws;

1.4.3 it is satisfied that:

(a) the Company's processing operations are suitable for the purposes for which the Customer proposes to use the Services and engage the Company to process the Protected Data; and

(b) the Company has sufficient expertise, reliability and resources to implement technical and organisational measures that meet the requirements of Data Protection Laws.

1.5 The Customer shall not unreasonably withhold, delay or condition its agreement to any Change requested by the Company in order to ensure the Services and the Company (and each Sub-Processor) can comply with Data Protection Laws.

2 Instructions and details of processing

2.1 Insofar as the Company processes Protected Data on behalf of the Customer, the Company:

2.1.1 unless required to do otherwise by Applicable Law, shall (and shall take steps to ensure each person acting under its authority shall) process the Protected Data only on and in accordance with the Customer's documented instructions as set out in this clause 2 and 0 (Data processing details), as updated from time to time in accordance with the Change Control Procedure (**Processing Instructions**);

2.1.2 if Applicable Law requires it to process Protected Data other than in accordance with the Processing Instructions, shall notify the Customer of any such requirement before processing the Protected Data (unless Applicable Law prohibits such information on important grounds of public interest); and

2.1.3 shall inform the Customer if the Company becomes aware of a Processing Instruction that, in the Company's opinion, infringes Data Protection Laws, provided that:

(a) this shall be without prejudice to clauses 1.3 and 1.4;

(b) to the maximum extent permitted by mandatory law, the Company shall have no liability howsoever arising (whether in contract, tort (including negligence) or otherwise) for any losses, costs, expenses or liabilities (including any Data Protection Losses) arising from or in connection with any processing in accordance with the Customer's Processing Instructions following the Customer's receipt of that information; and

(c) this clause 2.1.3 shall only apply from the GDPR Date.

2.2 The processing of Protected Data to be carried out by the Company under this Agreement shall comprise the processing set out in 0 (Data processing details), as may be updated from time to time in accordance with the Change Control Procedure.

3 Technical and organisational measures

3.1 The Company shall implement and maintain, at its cost and expense, the technical and organisational measures:

3.1.1 in relation to the processing of Protected Data by the Company, as set out in Appendix 2 (Technical and organisational measures); and

3.1.2 from the GDPR Date, taking into account the nature of the processing, to assist the Customer insofar as is possible in the fulfilment of the Customer's obligations to respond to Data Subject Requests relating to Protected Data.

3.2 Any additional technical and organisational measures shall be at the Customer's cost and expense.

4 Using staff and other processors

4.1 The Company shall appoint Sub-Processors under a written contract containing materially the same obligations as under clauses 1 to 11 (inclusive).

4.2 From the GDPR Date, the Company shall ensure that all Company Personnel authorised to process Protected Data are subject to a binding written contractual obligation with the Company to keep the Protected Data confidential (except where disclosure is required in accordance with Applicable Law, in which case the Company shall, where practicable and not prohibited by Applicable Law, notify the Customer of any such requirement before such disclosure).

5 Assistance with the Customer's compliance and Data Subject rights

5.1 The Company shall refer all Data Subject Requests it receives to the Customer within *three* Business Days of receipt of the request

5.2 From the GDPR Date, the Company shall provide such reasonable assistance as the Customer reasonably requires (taking into account the nature of processing and the information available to the Company) to the Customer in ensuring compliance with the Customer's obligations under Data Protection Laws with respect to:

5.2.1 security of processing;

5.2.2 data protection impact assessments (as such term is defined in Data Protection Laws);

5.2.3 prior consultation with a Supervisory Authority regarding high risk processing; and

5.2.4 notifications to the Supervisory Authority and/or communications to Data Subjects by the Customer in response to any Personal Data Breach,

6 Records, information and audit

6.1 The Company shall maintain, in accordance with Data Protection Laws binding on the Company, written records of all categories of processing activities carried out on behalf of the Customer.

6.2 The Company shall, in accordance with Data Protection Laws, make available to the Customer such information as is reasonably necessary to demonstrate the Company's compliance with the obligations of Data Processors under Data Protection Laws, and allow for and contribute to audits, including inspections, by the Customer (or another auditor mandated by the Customer) for this purpose, subject to the Customer:

6.2.1 giving the Company reasonable prior notice of such information request, audit and/or inspection being required by the Customer;

6.2.2 ensuring that all information obtained or generated by the Customer or its auditor(s) in connection with such information requests, inspections and audits is kept strictly confidential (save for disclosure to the Supervisory Authority or as otherwise required by Applicable Law);

6.2.3 ensuring that such audit or inspection is undertaken during normal business hours, with minimal disruption to the Company's business, the Sub-Processors' business and the business of other customers of the Company; and

6.2.4 paying the Company's reasonable costs for assisting with the provision of information and allowing for and contributing to inspections and audits.

7 Breach notification

7.1 In respect of any Personal Data Breach involving Protected Data, the Company shall, without undue delay:

7.1.1 notify the Customer of the Personal Data Breach; and

7.1.2 provide the Customer with details of the Personal Data Breach.

8 Deletion or return of Protected Data and copies

8.1 The Company shall, at the Customer's written request, either delete or return all the Protected Data to the Customer in such form as the Customer reasonably requests within a reasonable time after the earlier of:

8.1.1 the end of the provision of the relevant Services related to processing; or

8.1.2 once processing by the Company of any Protected Data is no longer required for the purpose of the Company's performance of its relevant obligations under this Agreement, and delete existing copies (unless storage of any data is required by Applicable Law and, if so, the Company shall inform the Customer of any such requirement).

8.2 From the GDPR Date, the Company shall implement a data retention policy. The Company's data retention policy will delete all of the Customer's client data when a client record reaches a state of having had **no update for 7 years.**

9 Indemnity and compensation claims

9.1 If a party receives a compensation claim from a person relating to processing of Protected Data, it shall promptly provide the other party with notice and full details of such claim. The party with conduct of the action shall:

9.1.1 make no admission of liability nor agree to any settlement or compromise of the relevant claim without the prior written consent of the other party (which shall not be unreasonably withheld or delayed); and

9.1.2 consult fully with the other party in relation to any such action.

9.2 The parties agree that the Customer shall not be entitled to claim back from the Company any part of any compensation paid by the Customer

10 Survival of data protection provisions

10.1 Clauses 1 to 9 (inclusive) shall survive termination (for any reason) or expiry of this Agreement and continue:

10.1.1 indefinitely in the case of clauses 7 to 9 (inclusive); and

10.1.2 until 12 months following the earlier of the termination or expiry of this Agreement in the case clauses 1 to 6 (inclusive), provided always that any termination or expiry of clauses 1 to 6 (inclusive) shall be without prejudice to any accrued rights or remedies of either party under any such clauses at the time of such termination or expiry.

1 Subject-matter of processing:

- The Customer's clients and any other individual's personal data that the Customer chooses to input into the proprietary software
- The Customer's user information

2 Duration of the processing:

For the duration of the contract between Eight Technology Ltd and the Customer

3 Nature and purpose of the processing:

The provision of proprietary software (Dealerweb Showroom & Dealerweb REACT) allowing Sales Teams to manage sales enquiries, customer contact, the creation and administration of sales transactions, FCA compliance support and Sales Activity Reporting

4 Type of Personal Data:

- FirstName
- Surname
- Postal Address (including postcode)
- Email
- Work Phone
- Home Phone
- Mobile Phone

5 Categories of Data Subjects:

- Customers
- System Users

6 Processing Instructions

Data will only be processed for the purposes of providing agreed services to the Customer

Eight Technology Ltd have an Information Security Management System (ISMS) in place conforming to ISO27001 standard and containing the following technical and organisational controls:

ISO27001:2013	Statement of Applicability (Annex A) For Eight Technology Ltd	
	This is a public version of the SOA released 19/4/2018	
5	**Information security policies**	**Applied**
5.1	**Management direction for information security**	
5.1.1	Policies for information security	Detailed in Eight Technology Information Security Polices
5.1.2	Review of the policies for information security	Detailed in Eight Technology ISO27001 Audit Plan
6	**Organisation of information security**	**Applied**
6.1	**Internal organisation**	
6.1.1	Information security roles and responsibilities	Defined in the Eight Technology Roles and responsibilities document
6.1.2	Segregation of duties	Defined in the Eight Technology Roles and responsibilities document
6.1.3	Contact with authorities	Defined in the Eight Technology Roles and responsibilities document
6.1.4	Contact with special interest groups	Defined in the Eight Technology Roles and responsibilities document
6.1.5	Information security in project management	Agenda item at the Eight Technology Security Steering group
6.2	**Mobile devices and teleworking**	
6.2.1	Mobile device policy	Defined in the Eight Technology Information Security Policy
6.2.2	Teleworking	Defined in the Eight Technology Information Security Policy
7	**Human resource security**	**Applied**
7.1	**Prior to Employment**	
7.1.1	Screening	Defined in HR Screening Policy
7.1.2	Terms and conditions of employment	Defined in the Eight Technology Employee Hand Book
7.2	**During employment**	
7.2.1	Management responsibilities	Defined in Roles and Responsibilities
7.2.2	Information security awareness, education and training	Defined as part of the HR Joiners policy, and Information Security Training Programm
7.2.3	Disciplinary process	Defined in the HR Policies
7.3	**Termination or change of employment**	
7.3.1	Termination or change of employment responsibilities	Defined in the HR Change of Role and Leavers Policy
8	**Asset management**	**Applied**
8.1	**Responsibility for assets**	
8.1.1	Inventory of assets	Detailed in the Eight Technology Asset register
8.1.2	Ownership of assets	Detailed in the Eight Technology Asset register
8.1.3	Acceptable use of assets	Defined in the Eight Technology Information Security Policy
8.1.4	Return of assets	Defined in the HR Leavers Policy

8.2	**Information classification**	
8.2.1	Classification of information	Defined in the Eight Technology Information Classification Matrix
8.2.2	Labelling of information	Defined in the Eight Technology Information Classification Matrix
8.2.3	Handling of assets	Defined in the Eight Technology Information Security Policy
8.3	**Media handling**	
8.3.1	Management of removable media	Defined in the Eight Technology Info Sec Manual
8.3.2	Disposal of media	Defined in the Eight Technology Info Sec Manual
8.3.3	Physical media transfer	Defined in the Eight Technology Info Sec Manual
9	**Access control**	**Applied**
9.1	**Business requirements for access control**	
9.1.1	Access control policy	Defined in the Eight Technology Information Security Policy
9.1.2	Access to networks and network services	Defined in the Eight Technology Information Security Policy
9.2	**User access management**	
9.2.1	User registration and deregistration	Defined in the HR Joiners and Leavers Policies
9.2.2	User access provisioning	Defined in the User Account Provisioning policy.
9.2.3	Management of privileged access rights	Defined in the User Account Provisioning Policy
9.2.4	Management of secret authentication information of users	Defined in the User Account Provisioning Policy
9.2.5	Review of user access rights	Defined in the User Account Provisioning Policy
9.2.6	Removal or adjustment of access rights	Defined in the HR Change of Role and Leavers Policy
9.3	**User responsibilities**	
9.3.1	Use of secret authentication information	Defined in the Eight Technology Information Security Policy
9.4	**System and application access control**	
9.4.1	Information access restriction	Defined in the User Account Provisioning policy.
9.4.2	Secure logon procedures	Defined in the Eight Technology Information Security Policy
9.4.3	Password management system	Defined in the Eight Technology Information Security Policy
9.4.4	Use of privileged utility programs	Defined in the Eight Technology Information Security Policy
9.4.5	Access control to program source code	Defined in the User Account Provisioning Policy
10	**Cryptography**	**Applied**
10.1	**Cryptographic controls**	
10.1.1	Policy on the use of cryptographic controls	Defined in the Eight Technology Information Security Policy
10.1.2	Key management	Defined in the Eight Technology Information Security Policy
11	**Physical and environmental security**	**Applied**
11.1	**Secure areas**	
11.1.1	Physical security perimeter	Physical Security provided by onsite security
11.1.2	Physical entry controls	Access control on all external doors.
11.1.3	Securing offices, rooms and facilities	Additional internal security controls within the Eight Technology office

11.1.4	Protecting against external and environmental threats	Business Continuity and Disaster Recovery plans in place
11.1.5	Working in secure areas	Additional internal security controls within the Eight Technology office
11.1.6	Delivery and loading areas	Physical Security provided by onsite security
11.2	**Equipment**	
11.2.1	Equipment siting and protection	Yes - In place
11.2.2	Supporting utilities	Business Continuity and Disaster Recovery plans in place
11.2.3	Cabling security	Yes - In place
11.2.4	Equipment maintenance	Defined in the Eight Technology refresh program
11.2.5	Removal of assets	Defined in the Eight Technology Information Security Policy
11.2.6	Security of equipment and assets off premises	Defined in the Eight Technology Information Security Policy
11.2.7	Secure disposal or reuse of equipment	Defined in the Eight Technology Security Policy
11.2.8	Unattended user equipment	Defined in the Eight Technology Information Security Policy
11.2.9	Clear desk and clear screen policy	Defined in the Eight Technology Information Security Policy
12	**Operations security**	**Applied**
12.1	**Operational procedures and responsibilities**	
12.1.1	Documented operating procedures	Defined in the Eight Technology Info Sec Manual
12.1.2	Change management	Defined in the Eight Technology Info Sec Manual
12.1.3	Capacity management	Defined in the Eight Technology Info Sec Manual
12.1.4	Separation of development, testing and operational environments	Defined in the Eight Technology Secure Development Policy
12.2	**Protection from malware**	
12.2.1	Controls against malware	Defined in the Eight Technology Info Sec Manual
12.3	**Backup**	
12.3.1	Information backup	Defined in the Eight Technology Info Sec Manual
12.4	**Logging and monitoring**	
12.4.1	Event logging	Defined in the Eight Technology Info Sec Manual
12.4.2	Protection of log information	Defined in the Eight Technology Info Sec Manual
12.4.3	Administrator and operator logs	Defined in the Eight Technology Info Sec Manual
12.4.4	Clock synchronisation	Defined in the Eight Technology Info Sec Manual
12.5	**Control of operational software**	
12.5.1	Installation of software on operational systems	Defined in the Eight Technology Information Security Policies -Software Installation
12.6	**Technical vulnerability management**	
12.6.1	Management of technical vulnerabilities	Defined in the Eight Technology Info Sec Manual
12.6.2	Restrictions on software installation	Defined in the Eight Technology Information Security Policies -Software Installation
12.7	**Information systems audit considerations**	

12.7.1	Information systems audit controls	Detailed in Eight Technology ISO27001 Audit Plan
13	**Communications security**	**Applied**
13.1	**Network security management**	
13.1.1	Network controls	Defined in the Eight Technology Information Security Policy and security manual
13.1.2	Security of network services	Defined in the Eight Technology Information Security Policy and security manual
13.1.3	Segregation in networks	Defined in the Eight Technology Information Security Policy and security manual
13.2	**Information transfer**	
13.2.1	Information transfer policies and procedures	Defined in the Eight Technology Info Sec Manual
13.2.2	Agreements on information transfer	Defined in the Eight Technology Info Sec Manual
13.2.3	Electronic messaging	Yes- Security controls in place
13.2.4	Confidentiality or non-disclosure agreements	Yes - In Place
14	**System acquisition, development and maintenance**	**Applied**
14.1	**Security requirements of information systems**	
14.1.1	Information security requirements analysis and specification	Defined in Eight Technology Secure Development Policy
14.1.2	Securing application services on public networks	Defined in Eight Technology Secure Development Policy
14.1.3	Protecting application services transactions	Defined in Eight Technology Secure Development Policy
14.2	**Security in development and support processes**	
14.2.1	Secure development policy	Defined in Eight Technology Secure Development Policy
14.2.2	System change control procedures	Defined in the Eight Technology Info Sec Manual
14.2.3	Technical review of applications after operating platform changes	Defined in the Eight Technology Info Sec Manual
14.2.4	Restrictions on changes to software packages	Defined in the Eight Technology Info Sec Manual
14.2.5	Secure system engineering principles	Defined in the Eight Technology Info Sec Manual
14.2.6	Secure development environment	Defined in Eight Technology Secure Development Policy
14.2.7	Outsourced development	Yes - Strict controls in place
14.2.8	System security testing	Defined in Eight Technology Secure Development Policy
14.2.9	System acceptance testing	Defined in Eight Technology Secure Development Policy
14.3	**Test data**	
14.3.1	Protection of test data	Defined in Eight Technology Secure Development Policy
15	**Supplier Relationships**	**Applied**
15.1	**Information security in supplier relationships**	
15.1.1	Information security policy for supplier relationships	Defined in Eight Technology Supplier Security Policy
15.1.2	Addressing security within supplier agreements	Defined in Eight Technology Supplier Security Policy
15.1.3	Information and communication technology supply chain	Detailed in the Eight Technology Third Party Supplier Register

15.2	**Supplier service delivery management**	
15.2.1	Monitoring and review of supplier services	Detailed in the Eight Technology Third Party Supplier Register
15.2.2	Managing changes to supplier services	Detailed in the Eight Technology Third Party Supplier Register
16	**Information security incident management**	**Applied**
16.1	**Management of information security incidents and improvements**	
16.1.1	Responsibilities and procedures	Defined in Roles and Responsibilities
16.1.2	Reporting information security events	Eight Technology Incident reporting procedure in place
16.1.3	Reporting information security weaknesses	Eight Technology Incident reporting procedure in place
16.1.4	Assessment of and decision on information security events	Eight Technology Incident reporting procedure in place
16.1.5	Response to information security incidents	Eight Technology Incident reporting procedure in place.
16.1.6	Learning from information security incidents	Eight Technology Incident reporting procedure in place. Reviewed at internal security steering group
16.1.7	Collection of evidence	Eight Technology Incident reporting procedure in place. Defined in roles and responsibilities
17	**Information security aspects of business continuity management**	**Applied**
17.1	**Information security continuity**	
17.1.1	Planning information security continuity	Business Continuity and Disaster Recovery plans in place and tested
17.1.2	Implementing information security continuity	Detailed in the Eight Technology Third Party Supplier Register
17.1.3	Verify, review and evaluate information security continuity	Detailed in the Eight Technology Third Party Supplier Register
17.2	**Redundancies**	
17.2.1	Availability of information processing facilities	Back up policies in place
18	**Compliance**	Applied
18.1	**Compliance with legal and contractual requirements**	
18.1.1	Identification of applicable legislation and contractual requirements	Detailed Eight Technology Legal Register in place
18.1.2	Intellectual property rights	Defined in Information Security Policy and included in staff training
18.1.3	Protection of records	Yes- Security controls in place
18.1.4	Privacy and protection of personally identifiable information	Yes - Compliance with Data Protection Act 1998 and GDPR
18.1.5	Regulation of cryptographic controls	Yes - In Place
18.2	**Information security reviews**	
18.2.1	Independent review of information security	Yes - In Place
18.2.2	Compliance with security policies and standards	Defined in Roles and Responsibilities
18.2.3	Technical compliance review	Detailed Eight Technology Penetration Test schedule in place