Crystaline Solutions GENERAL DATA PROTECTION POLICY

Crystaline Solutions Limited (or 'CSL', 'we', or 'our') sets out below its policy in relation to the general data protection regulations ((EU) 2016/679)

criminal records information	means personal information relating to criminal convictions and offences, allegations, proceedings, and related security measures;
data breach	means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal information;
data subject	means the individual to whom the personal information relates;
personal information	(sometimes known as personal data) means information relating to an individual who can be identified (directly or indirectly) from that information;
processing information	means obtaining, recording, organising, storing, amending, retrieving, disclosing and/or destroying information, or using or doing anything with it;
Pseudonymised	means the process by which personal information is processed in such a way that it cannot be used to identify an individual without the use of additional information, which is kept separately and subject to technical and organisational measures to ensure that the personal information cannot be attributed to an identifiable individual;
sensitive personal information	(sometimes known as 'special categories of personal data' or 'sensitive personal data') means personal information about an individual's race, ethnic origin, political opinions, religious or philosophical beliefs, trade union membership (or non-membership), genetics information, biometric information (where used to identify an individual) and information concerning an individual's health, sex life or sexual orientation.

1 Data protection principles

1.1 CSL will comply with the following data protection principles when processing personal information:

1.1.1 we will process personal information lawfully, fairly and in a transparent manner;

1.1.2 we will collect personal information for specified, explicit and legitimate purposes only, and will not process it in a way that is incompatible with those legitimate purposes;

1.1.3 we will only process the personal information that is adequate, relevant and necessary for the relevant purposes;

1.1.4 we will keep accurate and up to date personal information, and take reasonable steps to ensure that inaccurate personal information is deleted or corrected without delay;

1.1.5 we will keep personal information for no longer than is necessary for the purposes for which the information is processed; and

1.1.6 we will take appropriate technical and organisational measures to ensure that personal information is kept secure and protected against unauthorised or unlawful processing, and against accidental loss, destruction or damage.

F4 Silverbox House, 56 Magnet Road, Wembley HA9 7RG

2 Basis for processing personal information

2.1 In relation to any processing activity CSL will, before the processing starts for the first time, and then regularly while it continues:

2.1.1 review the purposes of the particular processing activity, and select the most appropriate lawful basis (or bases) for that processing, i.e.:

2.1.2 that the data subject has consented to the processing;

2.1.3 that the processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;

2.1.4 that the processing is necessary for compliance with a legal obligation to which CSL is subject that the processing is necessary for the purposes of legitimate interests of CSL or a third party, except where those interests are overridden by the interests of fundamental rights and freedoms of the data subject—see paragraph 2.2 below.

2.1.5 except where the processing is based on consent, satisfy ourselves that the processing is necessary for the purpose of the relevant lawful basis (i.e. that there is no other reasonable way to achieve that purpose);

2.1.6 document our decision as to which lawful basis applies, to help demonstrate our compliance with the data protection principles;

2.1.7 include information about both the purposes of the processing and the lawful basis for it in our relevant privacy notice(s).

2.2 When determining whether CSL's legitimate interests are the most appropriate basis for lawful processing, we will:

2.2.1 conduct a legitimate interests' assessment ('LIA') and keep a record of it, to ensure that we can justify our decision;

2.2.2 if the LIA identifies a significant privacy impact, consider whether we also need to conduct a data protection impact assessment ('DPIA');

2.2.3 keep the LIA under review, and repeat it if circumstances change; and

2.2.4 include information about our legitimate interests in our relevant privacy notice(s).

2.3 If we process sensitive personal information or criminal records information, we will keep written records of:

2.3.1 the relevant purpose(s) for which the processing takes place, including (where required) why it is necessary for that purpose;

2.3.2 the lawful basis for our processing; and

2.3.3 whether we retain and erase the personal information in accordance with our policy document and, if not, the reasons for not following our policy.

2.4 We will conduct regular reviews of the personal information we process and update our documentation accordingly. This may include:

2.4.1 carrying out information audits to find out what personal information CSL holds;

2.4.2 distributing questionnaires and talking to staff across CSL to get a more complete picture of our processing activities; and

F4 Silverbox House, 56 Magnet Road, Wembley HA9 7RG
Company Number: 07481633

2.4.3 reviewing our policies, procedures, contracts and agreements to address areas such as retention, security and data sharing.

3 Privacy notice

3.1 CSL will issue privacy notices from time to time, informing you about the personal information that we collect and hold relating to you, how you can expect your personal information to be used and for what purposes.

3.2 We will take appropriate measures to provide information in privacy notices in a concise, transparent, intelligible and easily accessible form, using clear and plain language.

3.3 You should contact Legal Counsel at **GDPR@CSLReality.com** if you are concerned or suspect that one of the following has taken place (or is taking place or likely to take place):

3.3.1 processing of personal data without a lawful basis for its processing or;

3.3.2 any data breach as set out in paragraph 6.1 below;

3.3.3 access to personal information without the proper authorisation;

3.3.4 personal information not kept or deleted securely;

3.3.5 removal of personal information, or devices containing personal information (or which can be used to access it), from CSL's premises without appropriate security measures being in place;

3.3.6 any other breach of this policy or of any of the data protection principles set out in paragraph 1.1 above.

4 Information security

4.1 CSL will use appropriate technical and organisational measures in accordance with our policies to keep personal information secure, and in particular to protect against unauthorised or unlawful
processing and against accidental loss, destruction or damage. These may include:

4.1.1 making sure that, where possible, personal information is pseudonymised or encrypted;

4.1.2 ensuring the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

4.1.3 ensuring that, in the event of a physical or technical incident, availability and access to personal information can be restored in a timely manner; and

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

4.2 Where CSL uses external organisations to process personal information on its behalf, we shall have a written contract with those external organisations with appropriate terms.

5 Storage and retention of personal information

5.1 Personal information (and sensitive personal information) will be kept securely in accordance with CSL's ***information security policy*.**

5.2 Personal information should not be retained for any longer than necessary. The length of time over which data should be retained will depend upon the circumstances, including the reasons why the personal information was obtained.

5.3 Personal information that is no longer required will be deleted permanently from our information systems and any hard copies will be destroyed securely.

6 Data breaches

6.1 A data breach may take many different forms, for example:

6.1.1 loss or theft of data or equipment on which personal information is stored;

6.1.2 unauthorised access to or use of personal information either by a member of staff or third party;

6.1.3 loss of data resulting from an equipment or systems (including hardware and software) failure;

6.1.4 human error, such as accidental deletion or alteration of data;

6.1.5 unforeseen circumstances, such as a fire or flood;

6.1.6 deliberate attacks on IT systems, such as hacking, viruses or phishing scams; and

6.1.7 'blagging' offences, where information is obtained by deceiving the organisation which holds it.

6.2 CSL will:

6.2.1 make the required report of a data breach to the Information Commissioner's Office without undue delay and, where possible within 72 hours of becoming aware of it, if it is likely to result in a risk to the rights and freedoms of individuals; and

6.2.2 notify the affected individuals if a data breach is likely to result in a high risk to their rights and freedoms and notification is required by law.

7 International transfers

7.1 CSL may transfer personal information outside the European Economic Area (EEA) (which comprises the countries in the USA on the basis that those companies have an adequate level of protection and safeguards, that they may have binding corporate rules or may be compliant with an approved code of conduct and have agreed to standard data protection clauses.

8 Training

CSL will ensure that staff are adequately trained regarding their data protection responsibilities. Individuals whose roles require regular access to personal information, or who are responsible for implementing this policy or responding to subject access requests under this policy, will receive additional training to help them understand their duties and how to comply with them.

9 Consequences of failing to comply

9.1 CSL takes compliance with this policy very seriously. Failure to comply with the policy:

9.1.1 puts at risk the individuals whose personal information is being processed; and

9.1.2 carries the risk of significant civil and criminal sanctions for the individual and CSL;

9.1.3 and may, in some circumstances, amount to a criminal offence by the individual.

9.2 Because of the importance of this policy, an employee's failure to comply with any requirement of it may lead to disciplinary action under our procedures, and this action may result in dismissal for gross misconduct. If a non-employee breaches this policy, they may have their contract terminated with immediate effect.

If you have any questions or concerns about anything in this policy, do not hesitate to contact CSL at **GDPR@CSLReality.co.uk**