## 1. Purpose

1.1 Crystallise Ltd ("the Company") is committed to the practice of responsible corporate behaviour and to complying with all laws, regulations and other requirements which govern the conduct of our operations.

1.2 The Company is fully committed to instilling a strong anti-corruption culture and is fully committed to compliance with all anti-bribery and anti-corruption legislation including, but not limited to, the Bribery Act 2010 ("the Act") and ensures that no bribes or other corrupt payments, inducements or similar are made, offered, sought or obtained by us or anyone working on our behalf.

## 2. Bribery

2.1 Bribery is defined as the giving or promising of a financial or other advantage to another party where that advantage is intended to induce the other party to perform a particular function improperly, to reward them for the same, or where the acceptance of that advantage is in itself improper conduct.

2.2 Bribery is also deemed to take place if any party requests or agrees to receive a financial or other advantage from another party where that advantage is intended to induce that party to perform a particular function improperly, where the acceptance of that advantage is in itself improper conduct, or where that party acts improperly in anticipation of such advantage.

2.3 Bribery of a foreign official is defined as the giving or promising of a financial or other advantage which is intended to influence the official in order to obtain business or an advantage in the conduct of business unless the foreign official is required or permitted by law to be influenced by such advantage.

## 3. Consequences of Bribery

3.1 Anyone or any organisation found guilty of bribery under the Act may face fines and/or prison terms. In addition, high legal costs and adverse publicity are likely to result from any breach of the Act.

3.2 For employees of the Company, failure to comply with this Policy and/or with the Act may result in:

3.2.1 disciplinary action which may include dismissal; and

3.2.2 criminal penalties under the Act which may result in a fine and/or imprisonment for up to 10 years.

3.3 For the Company, any breach of this Policy by any employee or business associate may result in:

3.3.1 the Company being deemed to be in breach of the Act;

3.3.2 the Company being subject to fines; and

3.3.3 the Company suffering negative publicity and further associated damage as a result of such breach.

## 4. Responsibility for Compliance and Scope of Policy

4.1 This Policy applies to all employees, agents, contractors, subcontractors, consultants, business partners and any other parties (including individuals, partnerships and bodies corporate) associated with the Company or any of its subsidiaries.

4.2 It is the responsibility of all of the abovementioned parties to ensure that bribery is prevented, detected and reported and all such reports should be made in accordance with the Company's Whistleblowing Policy or as otherwise stated in this Policy, as appropriate.

4.3 No party described in section 4.1 may:

4.3.1 give or promise any financial or other advantage to another party (or use a third party to do the same) on the Company's behalf where that advantage is intended to induce the other party to perform a particular function improperly, to reward them for the same, or where the acceptance of that advantage will in itself constitute improper conduct;

4.3.2 request or agree to receive any financial or other advantage from another party where that advantage is intended to induce the improper performance of a particular function, where the acceptance of that advantage will in itself constitute improper conduct, or where the recipient intends to act improperly in anticipation of such an advantage.

4.4 Parties described in section 4.1 must:

4.4.1 be aware and alert at all times of all bribery risks as described in this Policy and in particular as set out in section 9 below;

4.4.2 exercise due diligence at all times when dealing with third parties on behalf of the Company; and

4.4.3 report any and all concerns relating to bribery to your line manager or, in the case of non-employees, their normal point of contact within the Company, or otherwise in accordance with the Company's Whistleblowing Policy.

## 5. Facilitation Payments

5.1 A facilitation payment is defined as a small payment made to officials in order to ensure or speed up the performance of routine or necessary functions.

5.2 Facilitation payments constitute bribes and, subject to section 5.3, may not be made at any time irrespective of prevailing business customs in certain territories.

5.3 Facilitation or similar payments may be made in limited circumstances where your life is in danger but under no other circumstances. Any payment so made must be reported to your line manager as soon as is reasonably possible and practicable.

## 6. Gifts and Hospitality

6.1 Gifts and hospitality remain a legitimate part of conducting business and should be provided only in compliance with the Company's Gifts and Hospitality Policy.

6.2 Gifts and hospitality can, when excessive, constitute a bribe and/or a conflict of interest. Care and due diligence should be exercised at all times when giving or receiving any form of gift or hospitality on behalf of the Company.

6.3 The following general principles apply:

6.3.1 Gifts and hospitality may neither be given nor received as rewards, inducements or encouragement for preferential treatment or inappropriate or dishonest conduct.

6.3.2 Neither gifts nor hospitality should be actively sought or encouraged from any party, nor should the impression be given that the award of any business, custom, contract or similar will be in any way conditional on gifts or hospitality.

6.3.3 Cash should be neither given nor received as a gift under any circumstances.

6.3.4 Gifts and hospitality to or from relevant parties should be generally avoided at the time of contracts being tendered or awarded.

6.3.5 The value of all gifts and hospitality, whether given or received, should be proportionate to the matter to which they relate and should not be unusually high or generous when compared to prevailing practices in our industry or sector.

6.3.6 Certain gifts which would otherwise be in breach of this Policy and/or the Hospitality and Gifts Policy may be accepted if refusal would cause significant and/or cultural offence, however the Company will donate any gifts accepted for such reasons to a charity of the directors choosing.

6.3.7 All gifts and hospitality, whether given or received, must be recorded in the Hospitality & Gifts Register.

## 7. Charitable Donations

7.1 Charitable donations are permitted only to registered (non-profit) charities. No charitable donations may be given to any organisation which is not a registered charity.

7.2 All charitable donations must be fully recorded.

7.3 Proof of receipt of all charitable donations must be obtained from the recipient organisation.

7.4 Under no circumstances may charitable donations be made in cash.

7.5 No charitable donation may be made at the request of any party where that donation may result in improper conduct.

## 8. Political Donations

8.1 The Company does not make political donations and the Company is not affiliated with any political party, independent candidate, or with any other organisation whose activities are primarily political.

8.2 Employees and other associated parties are free to make personal donations provided such payments are not purported to be made on behalf of the Company and are not made to obtain any form of advantage in any business transaction.

## 9. Due Diligence and Risks

The following issues should be considered with care in any and all transactions, dealings with officials, and other business matters concerning third parties:

9.1 Territorial risks, particularly the prevalence of bribery and corruption in a particular country;

9.2 Cross-border payments, particularly those involving territories falling under section 9.1;

9.3 Requests for cash payment, payment through intermediaries or other unusual methods of payment;

9.4 Activities requiring the Company and / or any associated party to obtain permits or other forms of official authorisation;

9.5 Transactions involving the import or export of goods;

**This policy has been approved & authorised by:**

| | |
|---|---|
| **Name:** | Sue Martin |
| **Position:** | Director |
| **Date:** | 18/10/23 |
| **Signature:** |  |

Crystallise Ltd
Anti-Malware Policy
October 2023

## 1. Introduction

This document sets out the measures to be taken by Crystallise Ltd (the "Company"), and by all employees and authorised third parties with respect to the prevention, detection, and remedying of Malware on the Company's computer systems, devices, infrastructure, computing environment, and any and all other relevant equipment (collectively, "IT Systems").

## 2. Definitions

| | |
|---|---|
| **"IT Department"** | means the IT Manager and the IT Staff responsible for the administration, installation, and maintenance of the IT Systems **[**,-(Clevagroup) |
| **"IT Manager"** | means the manager of the IT Department, Chris Martin, chris.martin@crystalise.com; |
| **"IT Systems"** | means desktop and laptop computers, mobile devices, servers, networking equipment and other infrastructure, computing environment, and any and all other relevant equipment; |
| **"Malware"** | means (defined broadly) any type of malicious file, code, or software which performs malicious and unauthorised tasks including, but not limited to, deleting files, stealing data (personal and otherwise), gaining access to systems, changing device settings, and controlling devices and software. Types of malware include, but are not limited to, viruses, worms, trojans, rootkits, keyloggers, spyware, adware, phishing, and ransomware; and |
| **"User"** | means all employees and agents of the Company and any and all third parties authorised to use the IT Systems including, but not limited to, contractors,subscribers and sub-contractors. |

## 3. Scope and Key Principles

3.1 This Policy applies to all employees of the Company and any and all third parties authorised to use the IT Systems including, but not limited to, contractors,

subscribers and sub-contractors (collectively, “Users”). All Users must ensure that they are familiar with this Policy and must adhere to and comply with it at all times.

3.2 All Users must use the IT Systems only within the bounds of UK law and must not use the IT Systems for any purpose or activity which is likely to contravene any UK law whether now or in the future in force.

3.3 All Users must use the IT Systems in accordance with this Policy and all related Company Policies including, but not limited to, the IT Security Policy; Data Protection Policy; Access Control Policy; Communications, Email, Internet & Social Media Policy; and (where applicable) Bring Your Own Device (BYOD) Policy.

3.4 All line managers must ensure that Users under their control and direction adhere to and comply with this Policy at all times, as required under Paragraph 3.1.

3.5 This Policy outlines the measures and procedures taken by the Company to protect its IT Systems from Malware. This Policy promotes the use of anti-malware software on all IT Systems unless an exemption applies.

3.6 All Users are responsible for taking appropriate precautions to ensure the safe and secure use of IT Systems to reduce the risks of Malware being introduced onto any IT Systems, irrespective of the protections implemented under this Policy.

## 4. Client Device Protection

4.1 Unless an exemption applies, all devices that form part of, or are connected to, the IT Systems must have suitable anti-malware software installed and active.

4.2 All anti-malware software shall be kept up-to-date with the latest software updates and definitions. This process shall be performed automatically as determined by the software’s settings as set by the IT Department. Users shall not change such settings or attempt to cancel or delay any updates to anti-malware software save for optional delays in software prompts requiring the User to restart their computer or device, in which case, the User should save their work, close open applications, and restart their computer or device either as prompted or as soon as possible.

4.3 All IT Systems protected by anti-malware software shall be subject to a full system scan at least weekly. This process shall be performed automatically as determined by the software’s settings as set by the IT Department. Users shall not change such settings or attempt to cancel or delay scans save for optional delays in software prompts requiring the User to restart their computer or device, in which case, the User should save their work, close open applications, and restart their computer or device either as prompted or as soon as possible.

4.4 All IT Systems protected by anti-malware software shall have live scanning enabled. All files shall be scanned automatically when downloaded, copied, shared, or otherwise transferred onto a protected computer or device. All physical media (e.g., USB storage devices) shall be scanned automatically upon connection to a protected computer or device.

4.5 Any files being sent by email or being shared by other means including, but not limited to, messaging apps, shared cloud storage, or physical media, must be scanned for Malware before being sent or shared, or as part of the sending process, as appropriate.

## 5. Server Protection

5.1 All servers that form part of, or are connected to, the IT Systems must have suitable anti-malware and firewall software installed and active.

5.2 Suitable anti-malware solutions must be implemented at all internet and email gateways in order to prevent Malware from entering the IT Systems and Company network(s).

5.3 All anti-malware software shall be kept up-to-date with the latest software updates and definitions. This process shall be performed automatically as determined by the software's settings.

5.4 All IT Systems of this type protected by anti-malware software shall be subject to a full system scan at regular intervals. This process shall be performed automatically as determined by the software's settings.

5.5 All IT Systems of this type protected by anti-malware software shall have live scanning enabled. All files shall be scanned automatically when downloaded, copied, shared, or otherwise transferred onto a protected server, computer, or device. All physical media (e.g., USB storage devices) shall be scanned automatically upon connection to a protected server, computer, or device.

## 6. Users' Responsibilities

6.1 Where any Malware is detected by a User, this must be reported immediately to the IT Department (this rule shall apply even where the anti-malware software automatically fixes the problem). The IT Department shall promptly take any and all necessary action to remedy the situation. In limited circumstances, this may involve the temporary removal of the affected computer or device.

6.2 Users must immediately inform the IT Department (and, where such concerns relate to personal data, the Data Protection Officer) of any and all security concerns relating to the IT Systems.

6.3 If any Malware affects, is likely to affect, or is suspected to affect any personal data, in addition to the above, the issue must be reported immediately to the Data Protection Officer.

6.4 Users must immediately inform the IT Department of any other technical problems (including, but not limited to software errors) which may occur on the IT Systems.

6.5 Users must not attempt to bypass anti-malware software and attempt to open any files or run any software or code which the anti-malware software has blocked. If a User has a genuine business need to open such a file or run such software or code, they must first consult with the IT Department and approval, if granted, must be logged in writing. Any instructions given by the IT Department **OR** IT Manager with respect to the file, software, or code in question must be followed carefully (e.g., using a computer which is isolated from all other

IT Systems).

6.6 Where any User deliberately introduces any Malware to the IT Systems, this will constitute a breach of this Policy and a criminal offence under the Computer Misuse Act 1990 and will be handled as appropriate under the Company's disciplinary procedures.

## 7. Policy Review

The Company shall review this Policy not less than yearly and otherwise as required in order to ensure that it remains up-to-date and fit for purpose. All questions, concerns, and other feedback relating to this Policy should be communicated to the IT Manager, and/or the Data Protection Officer.

## 8. Implementation of Policy

This Policy shall be deemed effective as of 18th October 2023. No part of this Policy shall have retroactive effect and shall thus apply only to matters occurring on or after this date.

This Policy has been approved and authorised by:

| | |
|---|---|
| **Name:** | Sue Martin |
| **Position:** | Business Manager |
| **Date:** | 18th October 2023 |
| **Due for Review by:** | 31st January 2024 |
| **Signature:** |  |

# Crystallise Ltd Anti-Facilitation of Tax Evasion Policy

## Policy Statement

It is our policy to conduct all our business in an honest and ethical manner. We take a zero- tolerance approach to the facilitation of tax evasion, whether under UK, US, or any other applicable country's law.

As an employer, if we fail to prevent our employees, workers, agents, or service providers from facilitating tax evasion, we can face criminal sanctions including an unlimited fine, as well as exclusion from tendering for public contracts and damage to our reputation. We therefore take our legal responsibilities seriously.

To adhere to our responsibilities and address those risks we ask the following of Crystallise employees and business partners.

## Who does this policy apply to?

This policy applies to all persons working for Crystallise in any capacity, including all employees, agency workers, volunteers, interns, agents, contractors, external consultants, third-party representatives and business partners, sponsors, or any other person associated with us, wherever located.

## What is Tax Evasion and Tax Evasion Facilitation?

Tax evasion means the offense of cheating the public revenue or fraudulently evading UK tax and is a criminal offense. The offense requires an element of fraud, which means there must be deliberate action, or omission with dishonest intent.

- Foreign tax evasion means evading tax in a foreign country, provided that conduct is an offense in that country and would be a criminal offense if committed in the UK. As with tax evasion, the element of fraud means there must be deliberate action, or omission with dishonest intent; and Tax evasion facilitation means being knowingly concerned in, or taking steps with a view to, the fraudulent evasion of tax (whether UK tax or tax in a foreign country) by another person, or aiding, abetting, counselling or procuring the commission of that offense. Tax evasion facilitation

is a criminal offense, where it is done deliberately and dishonestly.

## What you must not do

It is not acceptable for you (or someone on your behalf) to:

- Engage in any form of facilitating tax evasion or foreign tax evasion;
- Aid, abet, counsel or procure the commission of a tax evasion offense or foreign tax evasion offense by another person;
- Fail to promptly report any request or demand from any third party to facilitate the fraudulent evasion of tax (whether UK tax or tax in a foreign country), or any suspected fraudulent evasion of tax (whether UK tax or tax in a foreign country) by another person, in accordance with this policy;
- Threaten or retaliate against another individual who has refused to commit a tax evasion offense or a foreign tax evasion offense or who has raised concerns under this policy.

## Your Responsibilities

The prevention, detection, and reporting of tax evasion and foreign tax evasion are the responsibility of all those working for or with Pearson. You are required to avoid any activity that *might* lead to, or suggest, a breach of this policy.

You must notify your line manager, or the Business Manager as soon as possible if you believe or suspect that a breach of this policy has occurred or may occur in the future.

Further "red flags" that may indicate potential tax evasion or foreign tax evasion are set out below.

## Potential Tax Evasion Red Flags

The following is a list of possible red flags that may raise concerns related to tax evasion or foreign tax evasion. The list is not intended to be exhaustive and is for illustrative purposes only.

- you become aware that a third party has made or intends to make a false statement relating to tax, has failed to disclose income or gains to, or to register with, HMRC (or the equivalent authority in any relevant non-UK jurisdiction), has delivered or intends to deliver a false document relating to tax, or has set up or intends to set up a structure to try to hide

income, gains or assets from a tax authority;

- you become aware that a third party has deliberately failed to register for VAT (or the equivalent tax in any relevant non-UK jurisdiction) or failed to account for VAT;
- a third-party requests payment in cash and/or refuses to sign a formal commission or fee agreement, or to provide an invoice or receipt for a payment made;
- you become aware that an employee asks to be treated as a self-employed contractor, but without any material changes to their working conditions;
- a supplier or other subcontractor is paid gross when they should have been paid net,
- a third-party requests that payment is made to a country or geographic location different from where the third-party resides or conducts business;
- a third party to whom we have provided services requests that their invoice is addressed to a different entity, where we did not provide services to such entity directly;
- a third party to whom we have provided services asks us to change the description of services rendered on an invoice in a way that seems designed to obscure the nature of the services provided;
- you receive an invoice from a third party that appears to be non-standard or customized;
- a third party insists on the use of contract amendments or refuses to put terms agreed in writing or asks for contracts or other documentation to be backdated;
- you notice that we have been invoiced for a commission or fee payment that appears too large or too small, given the service stated to have been provided;
- a third party requests or requires the use of an agent, intermediary, consultant, distributor or supplier that is not typically used by or known to us.

## How to Raise a Concern about Tax Evasion

You are encouraged to raise concerns about any issue or suspicion of tax evasion or foreign tax evasion at the earliest possible stage.

If you become aware of any fraudulent evasion of tax in the course of your work, or you are asked to assist another person in their fraudulent evasion of tax (whether directly or indirectly), or if you believe

or suspect that any fraudulent evasion of tax has occurred or may occur, the methods for raising a concern are noted below:

- Your Line Manager
- The Directors

If you are unsure about whether a particular act constitutes tax evasion or foreign tax evasion, raise it with your manager, or through the Directors as soon as possible.

You should note that the corporate offense is only committed where you deliberately and dishonestly take action to facilitate tax evasion or foreign tax evasion. However, a deliberate failure to report suspected tax evasion or foreign tax evasion, or "turning a blind eye" to suspicious activity could amount to criminal facilitation of tax evasion.

Crystallise Ltd has a strict policy of anti-retaliation towards those who raise concerns.

| | |
|---|---|
| Policy Owner: | Sue Martin |
| Policy Version: | Version 1 |
| Issue Date: | October 2023 |

# Crystallise Ltd
# Ethical Policy
October 23

## 1. Purpose

1.1 Crystallise Ltd ("the Company") is committed to the practice of responsible corporate behaviour.

1.2 Through its business practices the Company seeks to protect and promote the human rights and basic freedoms of all its employees and agents.

1.3 Further the Company is committed to protecting the rights of all of those whose work contributes to the success of the Company, including those employees and agents of suppliers to the Company.

1.4 The Company is also committed to eliminating bribery and corruption. It is essential that all employees and persons associated with the Company adhere to this policy and abstain from giving or receiving bribes of any form.

1.5 This policy is non-exhaustive, and all aspects of the Company's business should be considered in the spirit of this policy.

## 2. Human Rights

2.1 The Company is vehemently opposed to the use of slavery in all forms; cruel, inhuman or degrading punishments; and any attempt to control or reduce freedom of thought, conscience and religion.

2.2 The Company will ensure that all of its employees, agents and contractors are entitled to their human rights as set out in the Universal Declaration of Human Rights and the Human Rights Act 1998.

2.3 The Company will not enter into any business arrangement with any person, company or organisation which fails to uphold the human rights of its workers or who breach the human rights of those affected by the organisation's activities.

## 3. Workers' Rights

3.1 The Company is committed to complying with all relevant employment legislation and regulations. The Company regards such regulations and legislation as the minimum rather than the recommended standard.

3.2 No worker should be discriminated against on the basis of age, gender, race, sexual orientation, religion or beliefs, gender reassignment, marital status or pregnancy. All workers should be treated equally. Workers with the same experience and qualifications should receive equal pay for equal work.

3.3 No worker should be prevented from joining or forming a staff association or trade union, nor should any worker suffer any detriment as a result of joining, or failing to join, any such organisation.

3.4 Workers should be aware of the terms and conditions of their employment or

engagement from the outset. In particular workers must be made aware of the wage that they receive, when and how it is to be paid, the hours that they must work and any legal limit which exists for their protection and any overtime provisions. Workers should also be allowed such annual leave, sick leave, maternity / paternity leave and such other leave as is granted by legislation as a minimum.

3.5 The Company does not accept any corporal punishment, harassment in any form, or bullying in any form.

## 4. Environmental Issues

4.1 The Company is committed to keeping the environmental impact of its activities to a minimum and has established an Environmental Policy in order help achieve this aim.

4.2 As an absolute minimum, the Company will ensure that it meets all applicable environmental laws in whichever jurisdiction it may be operating.

## 5. Conflicts of Interest

5.1 The Company holds as fundamental to its success the trust and confidence of those with whom it deals, including clients, suppliers and employees. Conflicts of interest potentially undermine the relationship of the Company with its partners.

5.2 In order to help preserve and strengthen these relationships the Company has developed an Anti-Bribery Policy, which provide rules and guidelines concerning the conduct of its officers and employees aimed at minimising the possibility of conflicts of interest and at avoiding risks associated with bribery and corruption..

5.3 All officers, employees and representatives of the Company are expected to act honestly and within the law.

## 6. Information and Confidentiality

6.1. Information received by employees, contractors or agents of the Company will not be used for any personal gain, nor will it be used for any purpose beyond that for which it was given.

6.2 The Company will at all times ensure that it complies with all applicable requirements of the Data Protection Legislation. “Data Protection Legislation” means all applicable legislation in force from time to time in the United Kingdom applicable to data protection and privacy including, but not limited to, the UK GDPR (the retained EU law version of the General Data Protection Regulation ((EU) 2016/679), as it forms part of the law of England and Wales, Scotland, and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018); the Data Protection Act 2018 (and regulations made thereunder); and the Privacy and Electronic Communications Regulations 2003 as amended.

## 7. Shareholders and Investors

The Company, its officers, employees and representatives are committed to ensuring that no act or omission which is within their power and which would have the effect of deliberately, negligently or recklessly misleading the shareholders, creditors or other investors in the Company occurs.

## 8. Suppliers and Partners

8.1 The Company expects all suppliers and partners to work towards and uphold similar ethical and moral standards.

8.2 The Company will investigate the ethical record of potential new suppliers before entering into any agreement. Further, the Company reserves the right to request information from suppliers regarding the production and sources of goods supplied.

8.3 The Company reserves the right to withdraw from any agreement or other arrangement with any supplier or partner who is found to have acted in contravention of the spirit or principles of this Ethical Policy.

## 9. Bribery and Corruption

9.1 The Company is fundamentally opposed to any acts of bribery and to the making of facilitation payments as defined by the Bribery Act 2010.

9.2 Employees and any other persons associated with the Company such as agents, subsidiaries and business partners are not permitted to either offer or receive any type of bribe and/or facilitation payment.

9.3 All employees are encouraged to report any suspicion of corruption or bribery within the Company.

9.4 Should any employee or associated person be in doubt when receiving or issuing gifts and hospitality, he/she must refer to the Anti-Bribery Policy.

9.5 The Company uses its reasonable endeavours to implement the guidance principles on bribery management that are published, from time to time, by Secretary of State in accordance with Section 9 of the Bribery Act 2010.

9.6 If an employee or associated person is found guilty of giving or receiving a bribe, he/she will be personally criminally liable and may be subject to disciplinary action.

9.7 Anyone found guilty of bribery, will be responsible for bearing any related remedial costs such as losses, court fees or expenses.

**This policy has been approved & authorised by:**

| | |
|---|---|
| **Name:** | Sue Martin |
| **Position:** | Business Manager |
| **Date:** | 18th October 2023 |
| **Signature:** |  |

# Crystallise Ltd
# Corporate Social Responsibility Statement
October 2023

## 1. CSR Policy:

### 1.1 Introduction

We are, Crystallise Ltd. The prosperity of our business and of the communities within which we operate requires a commitment to the sustainable management of our activities. We have therefore developed a policy that affects and enhances all areas of our business.
We wish to adopt and commit to the principles and practices set out below.

### 1.2 Staff/People

We are committed to the well-being and continual development of our people and to training our workforce, where employees are appreciated, valued and given regular feedback so that each employee has a clear understanding of their role and how they contribute to the business.

We operate a meritocracy, where all employees are recognised on the basis of their performance, effort, contribution and achievements.

We expect our employees to act with integrity towards one another and exercise a high standard of business practice and workmanship.

We support diversity, fairness and equal opportunities and aim to involve and consult regularly with employees as to the direction of the business.

### 1.3 Customers

We aim to build long term relationships with all our customers and other stakeholders by understanding their objectives as they evolve over time and meeting their needs.
We aim to give fair value, consistent quality and reliability.

We aim to have the highest professional and ethical standards and will be honest, open and transparent in all our dealings with customers.

### 1.4 Suppliers

We aim to create and maintain strong relationships with key suppliers and contractors.
We aim to choose suppliers that share our ethos in relation to employment practices, quality and environmental controls. This will be communicated to all suppliers and potential suppliers.

### 1.5 Health & Safety

We aim to achieve and maintain the highest standards of health and safety and provide a safe and healthy working environment for all our activities.
We have a current and effective written health and safety policy that is regularly reviewed and updated.

### 1.6 Environment

We have implemented an environmental policy appropriate to our business.
We are aware of our environmental impact as a business and have taken and continue to take appropriate steps to mitigate that impact, including setting environmental objectives and targets, implementing procedures so employees and contractors understand their environmental responsibilities and can seek to improve our environmental performance.

## 1.7 **The Community**

We recognise and understand the significance of the local community within which we operate. We aim to enhance our contribution to the community by being sensitive to the needs of local people and groups and promoting ethical and socially responsible trading.

# Crystallise Ltd Data Protection Policy
## September 2022

1. **Introduction**

This Policy sets out the obligations of Crystallise Ltd, a company registered in England under number 07980921, whose registered office is at 17 High Street, Stanford-le-Hope, Essex SS17 0HD ("the Company") regarding data protection and the rights of Employees, Business Contacts, Customers and Suppliers ("data subjects") in respect of their personal data under Data Protection Law. "Data Protection Law" means all legislation and regulations in force from time to time regulating the use of personal data and the privacy of electronic communications including, but not limited to, the retained EU law version of the General Data Protection Regulation ((EU) 2016/679) (the "UK GDPR"), as it forms part of the law of England and Wales, Scotland, and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018, the Data Protection Act 2018, the Privacy and Electronic Communications Regulations 2003 as amended, and any successor legislation.

This Policy sets the Company's obligations regarding the collection, processing, transfer, storage, and disposal of personal data. The procedures and principles set out herein must be followed at all times by the Company, its employees, agents, contractors, or other parties working on behalf of the Company.

2. **Definitions**

| | |
|---|---|
| **"consent"** | means the consent of the data subject which must be a freely given, specific, informed, and unambiguous indication of the data subject's wishes by which they, by a statement or by a clear affirmative action, signify their agreement to the processing of personal data relating to them; |
| **"data controller"** | means the natural or legal person or organisation which, alone or jointly with others, determines the purposes and means of the processing of personal data. For the purposes of this Policy, the Company is the data controller of all personal data relating to Employees, Business Contacts, Customers and Suppliers used in our business for our commercial purposes; |
| **"data processor"** | means a natural or legal person or organisation which processes personal data on behalf of a data controller; |
| **"data subject"** | means a living, identified, or identifiable natural person about whom the Company holds personal data; |
| **"EEA"** | means the European Economic Area, consisting of all EU Member States, Iceland, Liechtenstein, and Norway; |
| **"personal data"** | means any information relating to a data subject who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, identification |

| | |
|---|---|
| | number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that data subject; |
| **"personal data breach"** | means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored, or otherwise processed; |
| **"processing"** | means any operation or set of operations performed on personal data or sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction; |
| **"pseudonymisation"** | means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data is not attributed to an identified or identifiable natural person; and |
| **"special category personal data"** | means personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, sexual life, sexual orientation, biometric, or genetic data. |

## 3. Scope

3.1 The Company is committed not only to the letter of the law, but also to the spirit of the law and places high importance on the correct, lawful, and fair handling of all personal data, respecting the legal rights, privacy, and trust of all individuals with whom it deals.

3.2 The Company's Data Protection Officer is Sue Martin, sue.martin@crystallise.com. The Data Protection Officer is responsible for administering this Policy and for developing and implementing any applicable related policies, procedures, and/or guidelines.

3.3 All Directors and line managers are responsible for ensuring that all employees, agents, contractors, or other parties working on behalf of the Company comply with this Policy and, where applicable, must implement such practices, processes, controls, and training as are reasonably necessary to ensure such compliance.

3.4 Any questions relating to this Policy or to Data Protection Law should be referred to the Data Protection Officer. In particular, the Data Protection Officer should always be consulted in the following cases:

a) if there is any uncertainty relating to the lawful basis on which personal data is to be collected, held, and/or processed;

b) if consent is being relied upon in order to collect, hold, and/or process personal data;

c) if there is any uncertainty relating to the retention period for any particular type(s) of personal data;

d) if any new or amended privacy notices or similar privacy-related documentation are required;

e) if any assistance is required in dealing with the exercise of a data subject's rights (including, but not limited to, the handling of subject access requests);

f) if a personal data breach (suspected or actual) has occurred;

g) if there is any uncertainty relating to security measures (whether technical or organisational) required to protect personal data;

h) if personal data is to be shared with third parties (whether such third parties are acting as data controllers or data processors);

i) if personal data is to be transferred outside of the UK and there are questions relating to the legal basis on which to do so;

j) when any significant new processing activity is to be carried out, or significant changes are to be made to existing processing activities, which will require a Data Protection Impact Assessment;

k) when personal data is to be used for purposes different to those for which it was originally collected;

l) if any automated processing, including profiling or automated decision-making, is to be carried out; or

m) if any assistance is required in complying with the law applicable to direct marketing.

## 4. The Data Protection Principles

This Policy aims to ensure compliance with Data Protection Law. The UK GDPR sets out the following principles with which any party handling personal data must comply. Data controllers are responsible for, and must be able to demonstrate, such compliance. All personal data must be:

4.1 processed lawfully, fairly, and in a transparent manner in relation to the data subject;

4.2 collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes. Further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;

4.3 adequate, relevant, and limited to what is necessary in relation to the purposes for which it is processed;

4.4 accurate and, where necessary, kept up to date. Every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the purposes for which it is processed, is erased, or rectified without delay;

4.5 kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed. Personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes, subject to implementation of the appropriate technical and organisational measures required by the UK GDPR

in order to safeguard the rights and freedoms of the data subject;

4.6 processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organisational measures.

## 5. The Rights of Data Subjects

The UK GDPR sets out the following key rights applicable to data subjects:

5.1 The right to be informed;

5.2 the right of access;

5.3 the right to rectification;

5.4 the right to erasure (also known as the 'right to be forgotten');

5.5 the right to restrict processing;

5.6 the right to data portability;

5.7 the right to object; and

5.8 rights with respect to automated decision-making and profiling.

## 6. Lawful, Fair, and Transparent Data Processing

6.1 Data Protection Law seeks to ensure that personal data is processed lawfully, fairly, and transparently, without adversely affecting the rights of the data subject. Specifically, the processing of personal data shall be lawful if at least one of the following applies:

a) the data subject has given consent to the processing of their personal data for one or more specific purposes;

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

c) the processing is necessary for compliance with a legal obligation to which the data controller is subject;

d) the processing is necessary to protect the vital interests of the data subject or of another natural person;

e) the processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the data controller; or

f) the processing is necessary for the purposes of the legitimate interests pursued by the data controller or by a third party, except where such interests are overridden by the fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

6.2 If the personal data in question is special category personal data (also known as "sensitive personal data"), at least one of the following conditions must be met:

a) the data subject has given their explicit consent to the processing of such data for one or more specified purposes (unless the law prohibits them from doing so);

b) the processing is necessary for the purpose of carrying out the obligations and exercising specific rights of the data controller or of the data subject in

the field of employment, social security, and social protection law (insofar as it is authorised by law or a collective agreement pursuant to law which provides for appropriate safeguards for the fundamental rights and interests of the data subject);

c) the processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;

d) the data controller is a foundation, association, or other non-profit body with a political, philosophical, religious, or trade union aim, and the processing is carried out in the course of its legitimate activities, provided that the processing relates solely to the members or former members of that body or to persons who have regular contact with it in connection with its purposes and that the personal data is not disclosed outside the body without the consent of the data subjects;

e) the processing relates to personal data which is manifestly made public by the data subject;

f) the processing is necessary for the conduct of legal claims or whenever courts are acting in their judicial capacity;

g) the processing is necessary for substantial public interest reasons, on the basis of law which shall be proportionate to the aim pursued, shall respect the essence of the right to data protection, and shall provide for suitable and specific measures to safeguard the fundamental rights and interests of the data subject;

h) the processing is necessary for the purposes of preventative or occupational medicine, for the assessment of the working capacity of an employee, for medical diagnosis, for the provision of health or social care or treatment, or the management of health or social care systems or services on the basis of law or pursuant to a contract with a health professional, subject to the conditions and safeguards referred to in Article 9(3) of the UK GDPR;

i) the processing is necessary for public interest reasons in the area of public health, for example, protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject (in particular, professional secrecy); or

j) the processing is necessary for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes in accordance with Article 89(1) of the UK GDPR (as supplemented by section 19 of the Data Protection Act 2018) based on law which shall be proportionate to the aim pursued, respect the essence of the right to data protection, and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

## 7. Consent

If consent is relied upon as the lawful basis for collecting, holding, and/or processing personal data, the following shall apply:

7.1 Consent is a clear indication by the data subject that they agree to the processing of their personal data. Such a clear indication may take the form of a statement or a positive action. Silence, pre-ticked boxes, or inactivity are unlikely to amount to consent.

7.2 Where consent is given in a document which includes other matters, the section dealing with consent must be kept clearly separate from such other matters.

7.3 Data subjects are free to withdraw consent at any time and it must be made easy for them to do so. If a data subject withdraws consent, their request must be honoured promptly.

7.4 If personal data is to be processed for a different purpose that is incompatible with the purpose or purposes for which that personal data was originally collected that was not disclosed to the data subject when they first provided their consent, consent to the new purpose or purposes may need to be obtained from the data subject.

7.5 If special category personal data is processed, the Company shall normally rely on a lawful basis other than explicit consent. If explicit consent is relied upon, the data subject in question must be issued with a suitable privacy notice in order to capture their consent.

7.6 In all cases where consent is relied upon as the lawful basis for collecting, holding, and/or processing personal data, records must be kept of all consents obtained in order to ensure that the Company can demonstrate its compliance with consent requirements.

## 8. Specified, Explicit, and Legitimate Purposes

8.1 The Company collects and processes the personal data set out in Part 24 of this Policy. This includes:

a) personal data collected directly from data subjects; and

b) personal data obtained from third parties.

8.2 The Company only collects, processes, and holds personal data for the specific purposes set out in Part 24 of this Policy (or for other purposes expressly permitted by Data Protection Law).

8.3 Data subjects must be kept informed at all times of the purpose or purposes for which the Company uses their personal data. Please refer to Part 15 for more information on keeping data subjects informed.

## 9. Adequate, Relevant, and Limited Data Processing

9.1 The Company will only collect and process personal data for and to the extent necessary for the specific purpose or purposes of which data subjects have been informed (or will be informed) as under Part 8, above, and as set out in Part 24, below.

9.2 Employees, agents, contractors, or other parties working on behalf of the Company may collect personal data only to the extent required for the performance of their job duties and only in accordance with this Policy. Excessive personal data must not be collected.

9.3 Employees, agents, contractors, or other parties working on behalf of the Company may process personal data only when the performance of their job duties requires it. Personal data held by the Company cannot be processed for any unrelated reasons.

## 10. Accuracy of Data and Keeping Data Up-to-Date

10.1 The Company shall ensure that all personal data collected, processed, and held by it is kept accurate and up to date. This includes, but is not limited to, the rectification of personal data at the request of a data subject, as set out in Part 17,

below.

10.2 The accuracy of personal data shall be checked when it is collected and at regular intervals thereafter. If any personal data is found to be inaccurate or out-of-date, all reasonable steps will be taken without delay to amend or erase that data, as appropriate.

## 11. Data Retention

11.1 The Company shall not keep personal data for any longer than is necessary in light of the purpose or purposes for which that personal data was originally collected, held, and processed.

11.2 When personal data is no longer required, all reasonable steps will be taken to erase or otherwise dispose of it without delay.

11.3 For full details of the Company's approach to data retention, including retention periods for specific personal data types held by the Company, please refer to our Data Retention Policy.

## 12. Secure Processing

12.1 The Company shall ensure that all personal data collected, held, and processed is kept secure and protected against unauthorised or unlawful processing and against accidental loss, destruction, or damage. Further details of the technical and organisational measures which shall be taken are provided in Parts 25 to 30 of this Policy.

12.2 All technical and organisational measures taken to protect personal data shall be regularly reviewed and evaluated to ensure their ongoing effectiveness and the continued security of personal data.

12.3 Data security must be maintained at all times by protecting the confidentiality, integrity, and availability of all personal data as follows:

a) only those with a genuine need to access and use personal data and who are authorised to do so may access and use it;

b) personal data must be accurate and suitable for the purpose or purposes for which it is collected, held, and processed; and

c) authorised users must always be able to access the personal data as required for the authorised purpose or purposes.

## 13. Accountability and Record-Keeping

13.1 The Data Protection Officer is responsible for administering this Policy and for developing and implementing any applicable related policies, procedures, and/or guidelines.

13.2 The Company shall follow a privacy by design approach at all times when collecting, holding, and processing personal data. Data Protection Impact Assessments shall be conducted if any processing presents a significant risk to the rights and freedoms of data subjects (please refer to Part 14 for further information).

13.3 All employees, agents, contractors, or other parties working on behalf of the Company shall be given appropriate training in data protection and privacy, addressing the relevant aspects of Data Protection Law, this Policy, and all other applicable Company policies.

13.4 The Company's data protection compliance shall be regularly reviewed and

evaluated by means of Data Protection Audits.

13.5 The Company shall keep written internal records of all personal data collection, holding, and processing, which shall incorporate the following information:

a) the name and details of the Company, its Data Protection Officer, and any applicable third-party data transfers (including data processors and other data controllers with whom personal data is shared);

b) the purposes for which the Company collects, holds, and processes personal data;

c) the Company's legal basis or bases (including, but not limited to, consent, the mechanism(s) for obtaining such consent, and records of such consent) for collecting, holding, and processing personal data;

d) details of the categories of personal data collected, held, and processed by the Company, and the categories of data subject to which that personal data relates;

e) details of any transfers of personal data to non-UK countries including all mechanisms and security safeguards;

f) details of how long personal data will be retained by the Company (please refer to the Company's Data Retention Policy);

g) details of personal data storage, including location(s);

h) detailed descriptions of all technical and organisational measures taken by the Company to ensure the security of personal data.

## 14. Data Protection Impact Assessments and Privacy by Design

14.1 In accordance with the privacy by design principles, the Company shall carry out Data Protection Impact Assessments for any and all new projects and/or new uses of personal data which involve the use of new technologies and where the processing involved is likely to result in a high risk to the rights and freedoms of data subjects.

14.2 The principles of privacy by design should be followed at all times when collecting, holding, and processing personal data. The following factors should be taken into consideration:

a) the nature, scope, context, and purpose or purposes of the collection, holding, and processing;

b) the state of the art of all relevant technical and organisational measures to be taken;

c) the cost of implementing such measures; and

d) the risks posed to data subjects and to the Company, including their likelihood and severity.

14.3 Data Protection Impact Assessments shall be overseen by the Data Protection Officer and shall address the following:

a) the type(s) of personal data that will be collected, held, and processed;

b) the purpose(s) for which personal data is to be used;

c) the Company's objectives;

d) how personal data is to be used;

e) the parties (internal and/or external) who are to be consulted;

f) the necessity and proportionality of the data processing with respect to the purpose(s) for which it is being processed;

g) risks posed to data subjects;

h) risks posed both within and to the Company; and

i) proposed measures to minimise and handle identified risks.

## 15. Keeping Data Subjects Informed

15.1 The Company shall provide the information set out in Part 15.2 to every data subject:

a) where personal data is collected directly from data subjects, those data subjects will be informed of its purpose at the time of collection; and

b) where personal data is obtained from a third party, the relevant data subjects will be informed of its purpose:

i) if the personal data is used to communicate with the data subject, when the first communication is made; or

ii) if the personal data is to be transferred to another party, before that transfer is made; or

iii) as soon as reasonably possible and in any event not more than one month after the personal data is obtained.

15.2 The following information shall be provided in the form of a privacy notice:

a) details of the Company including, but not limited to, contact details, and the names and contact details of any applicable representatives and its Data Protection Officer;

b) the purpose(s) for which the personal data is being collected and will be processed (as detailed in Part 24 of this Policy) and the lawful basis justifying that collection and processing;

c) where applicable, the legitimate interests upon which the Company is justifying its collection and processing of the personal data;

d) where the personal data is not obtained directly from the data subject, the categories of personal data collected and processed;

e) where the personal data is to be transferred to one or more third parties, details of those parties;

f) where the personal data is to be transferred to a third party that is located outside of the UK, details of that transfer, including but not limited to the safeguards in place (see Part 31 of this Policy for further details);

g) details of applicable data retention periods;

h) details of the data subject's rights under the UK GDPR;

i) details of the data subject's right to withdraw their consent to the Company's processing of their personal data at any time;

j) details of the data subject's right to complain to the Information Commissioner's Office;

k) where the personal data is not obtained directly from the data subject, details about the source of that personal data;

l) where applicable, details of any legal or contractual requirement or obligation necessitating the collection and processing of the personal data and details of any consequences of failing to provide it; and

m) details of any automated decision-making or profiling that will take place using the personal data, including information on how decisions will be made, the significance of those decisions, and any consequences.

## 16. Data Subject Access

16.1 Data subjects may make subject access requests ("SARs") at any time to find out more about the personal data which the Company holds about them, what it is doing with that personal data, and why.

16.2 Employees wishing to make a SAR should do using a Subject Access Request Form, sending the form to the Company's Data Protection Officer at sue.martin@crystallise.com.

16.3 Responses to SARs must normally be made within one month of receipt, however, this may be extended by up to two months if the SAR is complex and/or numerous requests are made. If such additional time is required, the data subject shall be informed.

16.4 All SARs received shall be handled by the Company's Data Protection Officer.

16.5 The Company does not charge a fee for the handling of normal SARs. The Company reserves the right to charge reasonable fees for additional copies of information that has already been supplied to a data subject, and for requests that are manifestly unfounded or excessive, particularly where such requests are repetitive.

## 17. Rectification of Personal Data

17.1 Data subjects have the right to require the Company to rectify any of their personal data that is inaccurate or incomplete.

17.2 The Company shall rectify the personal data in question, and inform the data subject of that rectification, within one month of the data subject informing the Company of the issue. The period can be extended by up to two months in the case of complex requests. If such additional time is required, the data subject shall be informed.

17.3 In the event that any affected personal data has been disclosed to third parties, those parties shall be informed of any rectification that must be made to that personal data.

## 18. Erasure of Personal Data

18.1 Data subjects have the right to request that the Company erases the personal data it holds about them in the following circumstances:

a) it is no longer necessary for the Company to hold that personal data with respect to the purpose(s) for which it was originally collected or processed;

b) the data subject wishes to withdraw their consent to the Company holding and processing their personal data;

c) the data subject objects to the Company holding and processing their personal data (and there is no overriding legitimate interest to allow the Company to continue doing so) (see Part 21 of this Policy for further details concerning the right to object);

d) the personal data has been processed unlawfully;

e) the personal data needs to be erased in order for the Company to comply with a particular legal obligation.

18.2 Unless the Company has reasonable grounds to refuse to erase personal data, all requests for erasure shall be complied with, and the data subject informed of the erasure, within one month of receipt of the data subject's request. The period can be extended by up to two months in the case of complex requests. If such additional time is required, the data subject shall be informed.

18.3 In the event that any personal data that is to be erased in response to a data subject's request has been disclosed to third parties, those parties shall be informed of the erasure (unless it is impossible or would require disproportionate effort to do so).

## 19. Restriction of Personal Data Processing

19.1 Data subjects may request that the Company ceases processing the personal data it holds about them. If a data subject makes such a request, the Company shall retain only the amount of personal data concerning that data subject (if any) that is necessary to ensure that the personal data in question is not processed further.

19.2 In the event that any affected personal data has been disclosed to third parties, those parties shall be informed of the applicable restrictions on processing it (unless it is impossible or would require disproportionate effort to do so).

## 20. Objections to Personal Data Processing

20.1 Data subjects have the right to object to the Company processing their personal data based on legitimate interests, for direct marketing (including profiling), and processing for scientific and/or historical research and statistics purposes.

20.2 Where a data subject objects to the Company processing their personal data based on its legitimate interests, the Company shall cease such processing immediately, unless it can be demonstrated that the Company's legitimate grounds for such processing override the data subject's interests, rights, and freedoms, or that the processing is necessary for the conduct of legal claims.

20.3 Where a data subject objects to the Company processing their personal data for direct marketing purposes, the Company shall cease such processing promptly.

20.4 Where a data subject objects to the Company processing their personal data for scientific and/or historical research and statistics purposes, the data subject must, under the UK GDPR, demonstrate grounds relating to his or her particular situation. The Company is not required to comply if the research is necessary for the performance of a task carried out for reasons of public interest.

## 21. Direct Marketing

21.1 The Company is subject to certain rules and regulations when marketing its products and services**.**

21.2 The prior consent of data subjects is required for electronic direct marketing including email, text messaging, and automated telephone calls subject to the following limited exception:

a) The Company may send marketing text messages or emails to a customer provided that that customer's contact details have been obtained in the course of a sale, the marketing relates to similar products or services, and the customer in question has been given the opportunity to opt-out of marketing when their details were first collected and in every subsequent communication from the Company.

21.3 The right to object to direct marketing shall be explicitly offered to data subjects in a clear and intelligible manner and must be kept separate from other information in order to preserve its clarity.

21.4 If a data subject objects to direct marketing, their request must be complied with promptly. A limited amount of personal data may be retained in such circumstances to the extent required to ensure that the data subject's marketing preferences continue to be complied with.

## 22. Personal Data Collected, Held, and Processed

The following personal data is collected, held, and processed by the Company (for details of data retention, please refer to the Company's Data Retention Policy):

| Data Ref. | Type of Data | Purpose of Data |
|---|---|---|
| A | Identity Data | First name, maiden name, last name, username or similar identifier |
| B | Contact Data | Personal, billing or delivery address and email addresses and telephone numbers. |
| C | Financial Data | Bank account and payment card details |
| D | Transaction Data | Including details about payments to and from you and other details of products and services you have purchased from us. |
| E | Technical Data | Includes internet protocol(IP) address, your login data, browser type and versions, operating system and platform and other technology on the devices you use to access our website. |
| F | Profile Data | Includes your username and password, purchases or orders made by you, your interests, preferences, feedback and survey responses |
| G | Usage Data | Includes information about how you use our website, products and services. |
| H | Marketing and Communications Data | Includes your preferences in receiving marketing from us and our third parties and your communication preferences |
| | | |

## 23. Data Security - Transferring Personal Data and Communications

The Company shall ensure that the following measures are taken with respect to all communications and other transfers involving personal data:

23.1 All emails containing personal data must be encrypted.

23.2 All emails containing personal data must be marked "confidential";

23.3 Personal data may be transmitted over secure networks only; transmission over unsecured networks is not permitted in any circumstances;

23.4 Personal data may not be transmitted over a wireless network if there is a wired alternative that is reasonably practicable;

23.5 Personal data contained in the body of an email, whether sent or received, should be copied from the body of that email and stored securely. The email itself should be deleted. All temporary files associated therewith should also be deleted.

23.6 Where personal data is to be sent by facsimile transmission the recipient should be informed in advance of the transmission and should be waiting by the fax machine to receive the data;

23.7 Where personal data is to be transferred in hardcopy form it should be passed directly to the recipient or sent using a signed for delivery service;

23.8 All personal data to be transferred physically, whether in hardcopy form or on removable electronic media shall be transferred in a suitable container marked “confidential”;

24. **Data Security - Storage**

The Company shall ensure that the following measures are taken with respect to the storage of personal data:

24.1 All electronic copies of personal data should be stored securely using passwords;

24.2 All hardcopies of personal data, along with any electronic copies stored on physical, removable media should be stored securely in a locked box, drawer, cabinet, or similar;

24.3 All personal data stored electronically should be backed up regularly with backups stored offsite. All backups should be encrypted.

24.4 No personal data should be stored on any mobile device (including, but not limited to, laptops, tablets, and smartphones), whether such device belongs to the Company or otherwise without the formal written approval of Sue Martin (Data Protection Officer) and, in the event of such approval, strictly in accordance with all instructions and limitations described at the time the approval is given, and for no longer than is absolutely necessary;

24.5 No personal data should be transferred to any device personally belonging to an employee, agent, contractor, or other party working on behalf of the Company and personal data may only be transferred to devices belonging to agents, contractors, or other parties working on behalf of the Company where the party in question has agreed to comply fully with the letter and spirit of this Policy and of the applicable Data Protection Law (which may include demonstrating to the Company that all suitable technical and organisational measures have been taken);

25. **Data Security - Disposal**

When any personal data is to be erased or otherwise disposed of for any reason (including where copies have been made and are no longer needed), it should be securely deleted and disposed of. For further information on the deletion and disposal of personal data, please refer to the Company’s Data Retention Policy.

26. **Data Security - Use of Personal Data**

The Company shall ensure that the following measures are taken with respect to the use of personal data:

26.1 No personal data may be shared informally and if an employee, agent, contractor, or other party working on behalf of the Company requires access to any personal data that they do not already have access to, such access should be formally requested from Sue Martin (Data Protection Officer).

26.2 No personal data may be transferred to any employee, agent, contractor, or other party, whether such parties are working on behalf of the Company or not, without the authorisation of Sue Martin (Data Protection Officer).

26.3 Personal data must be handled with care at all times and should not be left

unattended or on view to unauthorised employees, agents, contractors, or other parties at any time.

26.4 If personal data is being viewed on a computer screen and the computer in question is to be left unattended for any period of time, the user must lock the computer and screen before leaving it.

26.5 Where personal data held by the Company is used for marketing purposes, it shall be the responsibility of the Data Protection Officer to ensure that the appropriate consent is obtained and that no data subjects have opted out, whether directly or via a third-party service such as the TPS.

## 27. Data Security - IT Security

The Company shall ensure that the following measures are taken with respect to IT and information security:

27.1 All passwords used to protect personal data should be changed regularly and should not use words or phrases that can be easily guessed or otherwise compromised. All passwords must contain a combination of uppercase and lowercase letters, numbers, and symbols.;

27.2 Under no circumstances should any passwords be written down or shared between any employees, agents, contractors, or other parties working on behalf of the Company, irrespective of seniority or department. If a password is forgotten, it must be reset using the applicable method. IT staff do not have access to passwords;

27.3 All software (including, but not limited to, applications and operating systems) shall be kept up-to-date. The Company's IT staff shall be responsible for installing any and all security-related updates as soon as soon as reasonably and practically possible, unless there are valid technical reasons not to do so;

27.4 No software may be installed on any Company-owned computer or device without the prior approval of the Chris Martin.

## 28. Organisational Measures

The Company shall ensure that the following measures are taken with respect to the collection, holding, and processing of personal data:

28.1 All employees, agents, contractors, or other parties working on behalf of the Company shall be made fully aware of both their individual responsibilities and the Company's responsibilities under Data Protection Law and under this Policy, and shall be provided with a copy of this Policy;

28.2 Only employees, agents, contractors, or other parties working on behalf of the Company that need access to, and use of, personal data in order to carry out their assigned duties correctly shall have access to personal data held by the Company;

28.3 All sharing of personal data shall comply with the information provided to the relevant data subjects and, if required, the consent of such data subjects shall be obtained prior to the sharing of their personal data;

28.4 All employees, agents, contractors, or other parties working on behalf of the Company handling personal data will be appropriately trained to do so;

28.5 All employees, agents, contractors, or other parties working on behalf of the Company handling personal data will be appropriately supervised;

28.6 All employees, agents, contractors, or other parties working on behalf of the Company handling personal data shall be required and encouraged to exercise

care, caution, and discretion when discussing work-related matters that relate to personal data, whether in the workplace or otherwise;

28.7 Methods of collecting, holding, and processing personal data shall be regularly evaluated and reviewed;

28.8 All personal data held by the Company shall be reviewed periodically, as set out in the Company's Data Retention Policy;

28.9 The performance of those employees, agents, contractors, or other parties working on behalf of the Company handling personal data shall be regularly evaluated and reviewed;

28.10 All employees, agents, contractors, or other parties working on behalf of the Company handling personal data will be bound to do so in accordance with the principles of Data Protection Law and this Policy by contract;

28.11 All agents, contractors, or other parties working on behalf of the Company handling personal data must ensure that any and all of their employees who are involved in the processing of personal data are held to the same conditions as those relevant employees of the Company arising out of this Policy and Data Protection Law;

28.12 Where any agent, contractor or other party working on behalf of the Company handling personal data fails in their obligations under this Policy that party shall indemnify and hold harmless the Company against any costs, liability, damages, loss, claims or proceedings which may arise out of that failure;

## 29. Transferring Personal Data to a Country Outside the UK

29.1 The Company may, from time to time, transfer ('transfer' includes making available remotely) personal data to countries outside of the UK. The UK GDPR restricts such transfers in order to ensure that the level of protection given to data subjects is not compromised.

29.2 Personal data may only be transferred to a country outside the UK if one of the following applies:

a) The UK has issued regulations confirming that the country in question ensures an adequate level of protection (referred to as 'adequacy decisions' or 'adequacy regulations'). From 1 January 2021, transfers of personal data from the UK to EEA countries will continue to be permitted. Transitional provisions are also in place to recognise pre-existing EU adequacy decisions in the UK.

b) Appropriate safeguards are in place including binding corporate rules, standard contractual clauses approved for use in the UK (this includes those adopted by the European Commission prior to 1 January 2021), an approved code of conduct, or an approved certification mechanism.

c) The transfer is made with the informed and explicit consent of the relevant data subject(s).

d) The transfer is necessary for one of the other reasons set out in the UK GDPR including the performance of a contract between the data subject and the Company; public interest reasons; for the establishment, exercise, or defence of legal claims; to protect the vital interests of the data subject where the data subject is physically or legally incapable of giving consent; or, in limited circumstances, for the Company's legitimate interests.

30. **Data Breach Notification**

30.1 All personal data breaches must be reported immediately to the Company's Data Protection Officer.

30.2 If an employee, agent, contractor, or other party working on behalf of the Company becomes aware of or suspects that a personal data breach has occurred, they must not attempt to investigate it themselves. Any and all evidence relating to the personal data breach in question should be carefully retained.

30.3 If a personal data breach occurs and that breach is likely to result in a risk to the rights and freedoms of data subjects (e.g. financial loss, breach of confidentiality, discrimination, reputational damage, or other significant social or economic damage), the Data Protection Officer must ensure that the Information Commissioner's Office is informed of the breach without delay, and in any event, within 72 hours after having become aware of it.

30.4 In the event that a personal data breach is likely to result in a high risk (that is, a higher risk than that described under Part 32.3) to the rights and freedoms of data subjects, the Data Protection Officer must ensure that all affected data subjects are informed of the breach directly and without undue delay.

30.5 Data breach notifications shall include the following information:

a) The categories and approximate number of data subjects concerned;

b) The categories and approximate number of personal data records concerned;

c) The name and contact details of the Company's data protection officer (or other contact point where more information can be obtained);

d) The likely consequences of the breach;

e) Details of the measures taken, or proposed to be taken, by the Company to address the breach including, where appropriate, measures to mitigate its possible adverse effects.

31. **Implementation of Policy**

This Policy shall be deemed effective as of 1st September 2022. No part of this Policy shall have retroactive effect and shall thus apply only to matters occurring on or after this date.

This Policy has been approved and authorised by:

**Name:** Sue Martin

**Position:** Business Manager

**Date:** 01 September 2022

**Due for Review by:** 30 September 2023

**Signature:** 

Crystallise

# PRIVACY NOTICE

## BACKGROUND:

Crystallise Ltd. understands that your privacy is important to you and that you care about how your personal data is used. We respect and value the privacy of all of our colleagues and will only collect and use personal data in ways that are described here, and in a way that is consistent with our obligations and your rights under the law.

## 1. Information About Us

Crystallise Ltd. registered in England under company number 7980921.

Registered address: 17 High Steet, Stanford-le- Hope, Essex SS17 0HD

Main trading address: as above

VAT number: 190 8750 82

Contact: Sue Martin

Email address: sue.martin@crystallise.com

## 2. What Does This Notice Cover?

This Privacy Information explains how we use your personal data: how it is collected, how it is held, and how it is processed. It also explains your rights under the law relating to your personal data.

## 3. What is Personal Data?

Personal data is defined by the UK GDPR and the Data Protection Act 2018 (collectively, "the Data Protection Legislation") as 'any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier'.

Personal data is, in simpler terms, any information about you that enables you to be identified. Personal data covers obvious information such as your name and contact details, but it also covers less obvious information such as identification numbers, electronic location data, and other online identifiers.

The personal data that we use is set out in Part 5, below.

## 4. What Are My Rights?

Under the Data Protection Legislation, you have the following rights, which we will always work to uphold:

a) The right to be informed about our collection and use of your personal data. This Privacy Notice should tell you everything you need to know, but you can always contact us to find out more or to ask any questions using the details in Part 11.

b) The right to access the personal data we hold about you. Part 10 will tell you how to do this.

c) The right to have your personal data rectified if any of your personal data held by us is inaccurate or incomplete. Please contact us using the details in Part 11

to find out more.

d) The right to be forgotten, i.e. the right to ask us to delete or otherwise dispose of any of your personal data that we have. Please contact us using the details in Part 11 to find out more.

e) The right to restrict (i.e. prevent) the processing of your personal data.

f) The right to object to us using your personal data for a particular purpose or purposes.

g) The right to withdraw consent. This means that, if we are relying on your consent as the legal basis for using your personal data, you are free to withdraw that consent at any time.

h) The right to data portability. This means that, if you have provided personal data to us directly, we are using it with your consent or for the performance of a contract, and that data is processed using automated means, you can ask us for a copy of that personal data to re-use with another service or business in many cases.

i) Rights relating to automated decision-making and profiling. We do not use your personal data in this way.

For more information about our use of your personal data or exercising your rights as outlined above, please contact us using the details provided in Part 11.

Further information about your rights can also be obtained from the Information Commissioner's Office or your local Citizens Advice Bureau.

If you have any cause for complaint about our use of your personal data, you have the right to lodge a complaint with the Information Commissioner's Office.

## 5. What Personal Data Do You Collect?

We may collect some or all the following personal data (this may vary according to your relationship with us:

- Name;
- Address;
- Email address;
- Telephone number;
- Business name;
- Job title;
- Profession;
- Payment information.

## 6. How Do You Use My Personal Data?

Under the Data Protection Legislation, we must always have a lawful basis for using personal data. This may be because the data is necessary for our performance of a contract with you, because you have consented to our use of your personal data, or because it is in our legitimate business interests to use it. Your personal data may be used for one of the following purposes:

- Your personal details are required in order for us to enter into a contract with you.
- Communicating with you. This may include responding to emails or calls from you.

## 7. How Long Will You Keep My Personal Data?

We will not keep your personal data for any longer than is necessary in light of the reason(s) for which it was first collected. Your personal data will therefore be kept for the following periods (or, where there is no fixed period, the following factors will be used to determine how long it is kept):

- As long as a relationship for collaboration is in situ; or
- For 7 years after the termination of a business contract or employment with Crystallise Ltd.

## 8. How and Where Do You Store or Transfer My Personal Data?

We will only store or transfer your personal data in the UK. This means that it will be fully protected under the Data Protection Legislation.

## 9. Do You Share My Personal Data?

We will not share any of your personal data with any third parties for any purposes, subject to one important exception.

In some limited circumstances, we may be legally required to share certain personal data, which might include yours, if we are involved in legal proceedings or complying with legal obligations, a court order, or the instructions of a government authority.

## 10. How Can I Access My Personal Data?

If you want to know what personal data we have about you, you can ask us for details of that personal data and for a copy of it (where any such personal data is held). This is known as a “subject access request”.

All subject access requests should be made in writing and sent to the email or postal addresses shown in Part 11.

There is not normally any charge for a subject access request. If your request is ‘manifestly unfounded or excessive’ (for example, if you make repetitive requests) a fee may be charged to cover our administrative costs in responding.

We will respond to your subject access request within one month of receiving it. Normally, we aim to provide a complete response, including a copy of your personal data within that time. In some cases, however, particularly if your request is more complex, more time may be required up to a maximum of three months from the date we receive your request. You will be kept fully informed of our progress.

## 11. How Do I Contact You?

To contact us about anything to do with your personal data and data protection, including to make a subject access request, please use the following details:

Email address: sue.martin@crystallise.com

Postal Address: 17 High Street, Stanford-le-Hope, Essex SS17 0HD

## 12. Changes to this Privacy Notice

We may change this Privacy Notice from time to time. This may be necessary, for example, if the law changes, or if we change our business in a way that affects personal data protection.

Crystallise Ltd
Modern Slavery and Human Trafficking Statement
October 2023

## Introduction

This Modern Slavery and Human Trafficking Statement relates to actions and activities during the financial year 1st April 2022 t0 31st March 2023.

The statement sets down Crystallise Ltd's commitment to preventing slavery and human trafficking in our business activities and the steps we have put in place with the aim of ensuring that there is no slavery or human trafficking in our own business and supply chains. We all have a duty to be alert to risks, however small. Staff are expected to report their concerns and management to act upon them.

## Organisational structure and supply chains

This statement covers the business activities of Crystallise Ltd.

The Company currently operates in the following countries:

United Kingdom.

## High Risk Activities

The following activities are considered to be at high risk of modern slavery or human trafficking:

Crystallise Ltd's activities are not considered high risk.

Responsibility for the Company's anti-slavery initiatives is as follows:

- Policies: The Business Manager is responsible for creating and reviewing policies. The process by which policies are developed is looking at best practice and adapting to the needs of the Company.

- Due diligence: The Business Manager is responsible for due diligence in relation to known or suspected instances of modern slavery and human trafficking.

## Policies

The Company is committed to ensuring that there is no modern slavery or human trafficking in our business or our supply chains. This Statement affirms its intention to act ethically in our business relationships.

The following policies set down our approach to the identification of modern slavery risks and steps to be taken to prevent slavery and human trafficking in our operations:

- **Whistleblowing policy** - the Company encourages all its workers, customers and other business partners to report any concerns related to its direct activities or its supply chains.
- **Corporate Social Responsibility (CSR) Policy** - The Company's CSR policy summarises how we manage our environmental impacts and how we work responsibly with suppliers and local communities.

**Due Diligence Processes for Slavery and Human Trafficking**

The Company undertakes due diligence when considering taking on new suppliers, and regularly reviews its existing suppliers. The Company's due diligence process includes building long-standing relationships with suppliers and making clear our expectations of business partners and evaluating the modern slavery and human trafficking risks of each new supplier.

This Modern Slavery and Human Trafficking Statement will be regularly reviewed and updated as necessary. The Directors endorses this policy statement and is fully committed to its implementation.

This Modern Slavery and Human Trafficking Statement has been approved and authorised by:

| | |
|---|---|
| Name: | Sue Martin |
| Position: | Business Manager |
| Date: | 18th October 2023 |
| Signature: |  |