CONCISE SEPARATIONS
A CALIBRESCIENTIFIC COMPANY

Data Policy

CONTEXT AND OVERVIEW

Key details

- Policy prepared by: Dr Claire Naylor
- Approved by board/management on:
- Policy became operational on:
- Next review date: 7th February 2019

Introduction

CalibreScientific, Inc. needs to gather and use certain information about individuals.

These can include customers, suppliers, business contacts, employees and other people the organisation has a relationship with or may need to contact.

This policy describes how this personal data must be collected, handled and stored to meet the company's data protection standards – and to comply with the law.

Why this policy exists

This data protection policy ensures CalibreScientific:

- Complies with data protection law and follows good practice
- Protects the rights of staff, customers and partners
- Is open about how it stores and processes individuals' data
- Protects itself from the risks of a data breach

Data protection law

The Data Protection Act 1998 (and from 25th May 2018, the GDPR) describes how organisations – including CalibreScientific – must collect, handle and store personal information.

These rules apply regardless of whether data is stored electronically, on paper or on other materials,

To comply with the law, personal information must be collected and used fairly, stored safely and not disclosed unlawfully.

The Data Protection Act is underpinned by eight important principles. These say that personal data must:

1. Be processed fairly and lawfully
2. Be obtained only for specific, lawful purposes
3. Be adequate, relevant and not excessive
4. Be accurate and kept up to date
5. Not be held for any longer than necessary
6. Processed in accordance with the rights of data subjects
7. Be protected in Appropriate ways
8. Not be transferred outside the European Economic Area (EEA), unless that country or territory also ensures an adequate level of protection

p 844.348.4366

Concise Separations
2032 Concourse Drive
San Jose, CA 95131

W: conciseseparations.com

Data Policy

PEOPLE, RISKS AND RESPONSIBILITIES

Policy scope

This policy applies to:

- The head office CalibreScientific
- All portfolio companies of CalibreScientific
- All staff and volunteers of CalibreScientific
- All contractors, suppliers and other people working on behalf of CalibreScientific

It applies to all data that the company holds relating to identifiable individuals, even if that information technically falls outside of the Data Protection Act 1998. This can include:

- Names of individuals
- Postal addresses
- Email addresses
- Telephone numbers
- Any other information relating to individuals

Data protection risks

This policy helps to protect CalibreScientific from some very real data security risks, including:

- Breaches of confidentiality. For instance, information being given out inappropriately.
- Failing to offer choice. For instance, all individuals should be free to choose how the company uses data relating to them.
- Reputational damage. For instance, the company could suffer if hackers successfully gained access to sensitive data.

RESPONSIBILITIES

Everyone who works for or with CalibreScientific has some responsibility for ensuring data is collected, stored and handled appropriately.

Each team that handles personal data must ensure that it is handled and processed in line with this policy and data protection principles.

However, these people have key areas of responsibility:

- The Board of Directors is ultimately responsible for ensuring that CalibreScientific meets its legal obligations.
- The Data Protection Officer, Dr Claire Naylor, is responsible for:
  - Keeping the Board updated about data protection responsibilities, risks and issues.
  - Reviewing all data protection procedures and related policies, in line with an agreed schedule.
  - Arranging data protection training and advice for the people covered by this policy.
  - Handling data protection questions from staff and anyone else covered by this policy.

p 844.348.4366

Concise Separations
2032 Concourse Drive
San Jose, CA 95131

W: conciseseparations.com

- Dealing with requests from individuals to see the data CalibreScientific holds about them (also called 'subject access requests').
- Checking and approving any contracts or agreements with third parties that may handle the company's sensitive data.

- The IT and website support companies are responsible for:
  - Ensuring all systems, services and equipment used for storing data meet acceptable security standards.
  - Performing regular checks and scans to ensure security hardware and software is functioning properly.
- The Marketing Manager, Dr Claire Naylor, is responsible for:
  - Approving any data protection statements attached to communications such as emails and letters.
  - Addressing any data protection queries from journalists or media outlets like newspapers.
  - Where necessary, working with other staff to ensure marketing initiatives abide by data protection principles.
  - Evaluating any third-party services the company is considering using to store or process data. For instance, cloud computing services.

GENERAL STAFF GUIDELINES

- The only people able to access data covered by this policy should be those who need it for their work.
- Data should not be shared informally. When access to confidential information is required, employees can request it from their line managers.
- CalibreScientific will provide training to all employees to help them understand their responsibilities when handling data.
- Employees should keep all data secure, by taking sensible precautions and following the guidelines below.
- In particular, strong passwords must be used and they should never be shared.
- Personal data should not be disclosed to unauthorised people, either within the company or externally.
- Data should be regularly reviewed and updated if it is found to be out of date. If no longer required, it should be deleted and disposed of.
- Employees should request help from their line manager or the data protection officer if they are unsure about any aspect of data protection.

DATA STORAGE

These rules describe how and where data should be safely stored. Questions about storing data safely can be directed to the IT manager or data controller.

When data is stored on paper, it should be kept in a secure place where unauthorised people cannot see it.

These guidelines also apply to data that is usually stored electronically but has been printed out for some reason:

- When not required, the paper or files should be kept in a locked drawer or filing cabinet.
- Employees should make sure paper and printouts are not left where unauthorised people could see them, like on a printer.

- Data printouts should be shredded and disposed of securely when no longer required.

When data is stored electronically, it must be protected from unauthorised access, accidental deletion and malicious hacking attempts:

- Data should be protected by strong passwords that are changed regularly and never shared between employees.
- If data is stored on removable media (like a CD or DVD), these should be kept locked away securely when not being used.
- Data should only be stored on designated drives and servers, and should only be uploaded to an approved cloud computing services.
- Servers containing personal data should be sited in a secure location, away from general office space.
- Data should be backed up frequently. Those backups should be tested regularly, in line with the company's standard backup procedures.
- Data should never be saved directly to laptops or other mobile devices like tablets or smart phones.
- All servers and computers containing data should be protected by approved security software and a firewall.

DATA USE

Personal data is of no value to CalibreScientific unless the business can make use of it. However, it is when personal data is accessed and used that it can be at the greatest risk of loss, corruption or theft:

- When working with personal data, employees should ensure the screens of their computers are always locked when left unattended.
- Personal data should not be shared informally. In particular, it should never be sent by email, as this form of communication is not secure.
- Data must be encrypted before being transferred electronically. The IT manager can explain how to send data to authorised external contacts.
- Personal data should never be transferred outside of the European Economic Area.
- Employees should not save copies of personal data to their own computers. Always access and update the central copy of any data.

DATA ACCURACY

The law requires CalibreScientific to take reasonable steps to ensure data is kept accurate and up to date.

The more important it is that the personal data is accurate, the greater the effort CalibreScientific should put into ensuring its accuracy.

It is the responsibility of all employees who work with data to take reasonable steps to ensure it is kept as accurate and up to date as possible.

- Data will be held in as few places as necessary. Staff should not create any unnecessary additional data sets.
- Staff should take every opportunity to ensure data is updated. For instance, by confirming a customer's details when they call.
- CalibreScientific will make it easy for data subjects to update the information CalibreScientific holds about them. For instance, via the company website.

- Data should be updated as inaccuracies are discovered. For instance, if a customer can no longer be reached on their stored telephone number, it should be removed from the database.
- It is the marketing manager's responsibility to ensure marketing databases are checked against industry suppression files every six months.

SUBJECT ACCESS REQUESTS (SAR)

All individuals who are the subject of personal data held by CalibreScientific are entitled to:

- Ask what information the company holds about them and why.
- Ask how to gain access to it.
- Be informed how to keep it up to date.
- Be informed how the company is meeting its data protection obligations.
- Ask to have their information deleted.
- Request that no further contact occur.

If any individual contacts the company requesting this information, this is called a subject access request.

Subject access requests from individuals should be made by email, addressed to the data controller at enquiries@moleculardimensions.com. The data controller can supply a standard request form, although individuals do not have to use this. The data controller will aim to provide the relevant data within 14 days.

The data controller will always verify the identity of anyone making a subject access request before handing over any information.

DISCLOSING DATA FOR OTHER REASONS

In certain circumstances, the Data Protection Act (and the GDPR from 25th May 2018) allows personal data to be disclosed to law enforcement agencies without the consent of the data subject.

Under these circumstances, CalibreScientific will disclose requested data. However, the data controller will ensure the request is legitimate, seeking assistance from the board and from the company's legal advisers where necessary.

PROVIDING INFORMATION

CalibreScientific aims to ensure that individuals are aware that their data is being processed, and that they understand:

- How the data is being used
- How to exercise their rights

To these ends, the company has a privacy statement, setting out how data relating to individuals is used by the company.

[This is available on request. A version of this statement is also available on the company's website.]

Privacy Policy

CalibreScientific, Inc. respects your concerns about privacy.

CalibreScientific is made up of different legal entities, details of which can be found here: https://calibrescientific.com/. This privacy policy is issued on behalf of the CalibreScientific Group so when we mention "CalibreScientific", "we", "us" or "our" in this privacy notice, we are referring to the relevant company in the CalibreScientific Group responsible for processing your data. We will let you know which entity will be the controller when you purchase a product or service with us. CalibreScientific, Inc. is the controller and responsible for this website.

We have appointed a group data protection officer ("DPO") who is responsible for overseeing questions in relation to this privacy notice. If you have any questions about this privacy notice, including any requests to exercise your legal rights, please contact the DPO at: enquiries@moleculardimensions.com

This privacy policy describes how we collect, use, share and protect your personal information and your rights regarding our use.

Information We Collect

CalibreScientific may collect personally identifiable information including:

- Personal and business contact information (such as name, postal/email address, and telephone number)
- Other personal information you submit to us that is relevant to our business services such as information you provide to register for email alerts

Information We Obtain by Automated Means

Cookies are text files placed on your computer or other internet-connected device to uniquely identify your browser. CalibreScientific, and certain third-party web provides, may use these and/or similar technology in order to obtain marketing and website analytics. In the event of third-party use information will be disclosed and/or collected by these service providers.

You may choose to block or delete cookies from your browser.

For additional information on cookies please visit www.aboutcookies.org or www.allaboutcokies.org.

Data Retention

We will only retain your personal data for as long as necessary to fulfil the purposes we collected it for, including for the purposes of satisfying any legal, accounting, or reporting requirements.

To determine the appropriate retention period for personal data, we consider the amount, nature, and sensitivity of the personal data, the potential risk of harm from unauthorized use or disclosure of your personal data, the purposes for which we process your personal data and whether we can achieve those purposes through other means, and the applicable legal requirements.

Data Security

We have put in place appropriate security measures to prevent your personal data from being accidentally lost, used or accessed in an unauthorized way, altered or disclosed. In addition, we limit access to your personal data to those employees, agents, contractors

and other third parties who have a business need to know. They will only process your personal data on our instructions and they are subject to a duty of confidentiality.

We have put in place procedures to deal with any suspected personal data breach and will notify you and any applicable regulator of a breach where we are legally required to do so.

Use of and Purposes for Processing Personal Data

CalibreScientific processes your personal data in order to comply with our legal and regulatory obligations, our contractual obligations to provide our programs and services to you and/or the legitimate interests of CalibreScientific, and for other purposes for which CalibreScientific has a lawful basis under applicable law, including but not limited to: (i) providing our goods and services; (ii) responding to your inquiries; (iii) performing regular business operations; (iv) complying with legal and regulatory requirements; and (iv) participating in litigation, investigations, regulatory or governmental enquiries or for other legal or regulatory purposes involving CalibreScientific.

If you provide your email address, we may use your email address to send you promotional materials, newsletters and other communications. If you wish to opt out of promotional emails, you may do so by following the "unsubscribe" instructions in the email.

How We Share Collected Information

CalibreScientific may disclose your personal information with contracted third parties who require the data to perform services based on our legitimate business interests, contractual obligations or with our legal and regulatory requirements.

If you consent, we may share your personal information with our affiliates and subsidiaries so that they may contact you regarding their products and services. If you have consented, you have the right to opt out from marketing communications at a later date.

Data Transfers

Personal information may be transferred to recipients in countries that may not have the same data protection laws as the country in which the information was originally shared. In the event of a transfer, we will ensure data is processed with an adequate level of protection.

Except for those circumstances where we believe that it is appropriate to rely on contractual necessity or your express consent, whenever we transfer your personal data out of the European Economic Area (the "EEA"), we ensure a similar degree of protection is afforded to it by using specific contracts approved by the European Commission which give personal data the same level of protection as it has in the EEA. Please contact us if you require further information on the specific mechanism used by us when transferring your personal data.

Your Rights

You have the right to:

- Request access to your personal data (commonly known as a "data subject access request"). This enables you to receive a copy of the personal data we hold about you and to check that we are lawfully processing it
- Request correction of the personal data that we hold about you. This enables you to have any incomplete or inaccurate data we

hold about you corrected, though we may need to verify the accuracy of the new data you provide to us.

- Request erasure of your personal data. This enables you to ask us to delete or remove personal data where there is no good reason for us continuing to process it. You also have the right to ask us to delete or remove your personal data where you have successfully exercised your right to object to processing (see below), where we may have processed your information unlawfully or where we are required to erase your personal data to comply with local law. Note, however, that we may not always be able to comply with your request of erasure for specific legal reasons which will be notified to you, if applicable, at the time of your request.
- Object to processing of your personal data where we are relying on a legitimate interest (or those of a third party) and there is something about your particular situation which makes you want to object to processing on this ground as you feel it impacts on your fundamental rights and freedoms. You also have the right to object where we are processing your personal data for direct marketing purposes. In some cases, we may demonstrate that we have compelling legitimate grounds to process your information which override your rights and freedoms.
- Request restriction of processing of your personal data. This enables you to ask us to suspend the processing of your personal data in the following scenarios: (a) if you want us to establish the data's accuracy; (b) where our use of the data is unlawful but you do not want us to erase it; (c) where you need us to hold the data even if we no longer require it as you need it to establish, exercise or defend legal claims; or (d) you have objected to our use of your data but we need to verify whether we have overriding legitimate grounds to use it.
- Request the transfer of your personal data to you or to a third party. We will provide to you, or a third party you have chosen, your personal data in a structured, commonly used, machine-readable format. Note that this right only applies to automated information which you initially provided consent for us to use or where we used the information to perform a contract with you.
- Withdraw consent at any time where we are relying on consent to process your personal data. However, this will not affect the lawfulness of any processing carried out before you withdraw your consent. If you withdraw your consent, we may not be able to provide certain products or services to you. We will advise you if this is the case at the time you withdraw your consent.

You have the right to make a complaint at any time to a supervisory authority in your country. We would, however, appreciate the chance to deal with your concerns before you approach the supervisory authority so please contact us in the first instance.

Access to Your Information

To the extent provided by the law of your jurisdiction, you may request:

- A copy of the data we have on file
- To amend, delete or block information
- To withdraw consent previously provided
- To object, on a legitimate basis, to the processing of your personal information

To update your preferences or submit a request, please contact us as indicated in the "How to Contact Us" section of this Privacy Policy.

Other websites

Links on our site may lead to outside sources with their own privacy notices or policies, which we suggest you review. The practices outlined in this privacy policy pertain solely to the CalibreScientific site.

Privacy Policy Updates

Our privacy policy may be updated periodically and without prior notice to you. All changes will be posted on the CalibreScientific website.

How to Contact Us

If you have questions, comments, concerns or request related to your personal information please contact us using one of the following methods:

- Email: inquiries@calibrescientific.com
- Telephone: +1 (310) 774-0014
- Mail: CalibreScientific Data Compliance
  2049 Century Park East, Suite 2550
  Los Angeles, CA 90067 USA