Data Protection Policy

DACTEC Ltd

May 2018

Statement of Policy

DACTEC Ltd aims to achieve the best possible standards of protection for all the data, including personal data, which it collects and processes. It is committed to compliance with the requirements of the Data Protection Acts and the General Data Protection Regulations of May 2018.

DACTEC Ltd recognises its responsibilities, and will comply with, all relevant statutory legal requirements. It recognises its obligations to manage and achieve adequate standards of Data Protection on behalf of any Customers, Suppliers, employees or others, who provide it with Personal Data. It recognises its responsibilities in terms of the collection of, storage of, retention of, sharing of, providing access to and the correction of inaccurate information. It recognises the rights of individual data subjects to access to, to correction of, deletion of or portability of their data, and will comply with the GDPR in this regard – or will provide a full explanation where any conflict arises as set out in this policy.

It will carry out a regular audit of the types of personal data which it holds and processes. It will assess the risks associated with the data it processes and will take the necessary measures to keep it safe and to comply with the legislation. It will provide appropriate instruction, training, information and supervision of any person who may process the data. It will provide for review periodically, in light of experience and changing circumstances in the future, but at least annually.

The legal basis for the processing of data in DACTEC Ltd is by explicit consent and as a necessary requirement for the provision of Customer support. The processing may also comply with the legitimate interests of the DACTEC Representative and the employee (employment contracts).

The purpose of collecting personal data from Customers is to use this to communicate with them and support them with their chamber needs.

The data may be stored in a variety of means as set out in this policy. All data is kept secure and considered confidential. Data may be shared with chamber manufacturers and will only be shared with other third parties with the written consent of the data subject as set out in this policy.

The retention period for personal data is normally 10 years except in exceptional circumstances.

It is recognised that in co-operating with this policy Customers, employees and others will comply with the requirements of this policy. They will report any concerns about data protection to the company without delay so that such concerns can be investigated.

Signed: _____ Date: 25th May 2018

David Toner M.D and Data Protection Officer, DACTEC Ltd.

DACTEC Ltd Profile

DACTEC Ltd is an Irish based and owned Company founded in 2008. It sells and supports production and test chambers.

The Customer and Supplier personal data we collect is as follows:

1. Office phone numbers.
2. Company Email addresses.
3. In some cases personal mobile numbers.

The Employee personal data we hold consists of address and phone numbers. All Employees are members of DACTEC's owning family.

Employment Details

The DACTEC Ltd employs 1 person full time, the owner and M.D. Other staff include one part-time Administrator and two part time and seasonal apprentices.

Employee, Contractors, Suppliers and Customerss Co-operation

All DACTEC staff, Customers and Suppliers, will co-operate fully with the arrangements made by DACTEC Ltd, as set out in this policy, for the protection of Personal Data.

Anyone with concerns about Data Protection issues should immediately report all such concerns to the M.D., so that they can be investigated and acted upon appropriately without delay.

Any employee, or other person, is expected to comply with the requirements of this policy so that DACTEC Ltd may remain compliant with the Data Protection Acts and the GDPR.

Any employee, and other person, is expected to avoid causing a breach of Data Protection by any of their actions.

Any employee, working as a data processor, is reminded that they have specific statutory responsibilities under the Data Protection Acts and the GDPR.

Compliance & Disciplinary Policy

When advice and persuasion fail, and Customer, Supplier, an employee, or other person continues to fail to comply with the requirements of the Data Protection Policy, it is the policy of DACTEC Ltd to pursue the matter through an appropriate disciplinary code or other appropriate action.

Compliance with the arrangements set out in this Data Protection Policy is required of all employees, Customers and Suppliers.

Compliance with the arrangements set out in this Data Protection Policy will be a requirement of securing contracts / the provision of services or products. Where a Supplier fails to comply with, or to heed, representations made to him / her by the M.D., then DACTEC Ltd may seek to cancel the contract forthwith.

Communication + Consultation

A statement of Policy will be prominently displayed in the office area.

The Data Controller for this business is the M.D..

All personal Data is collected and used for the purposes of support of the Customers.

Customers, Suppliers or others with any concerns about matters related to Data Protection should discuss these directly with the M.D., who is the Data Controller, and as such has the ultimate responsibility for such matters.

For the purposes of this policy the Data Protection Officer is also DACTEC's Data Controller as it a small business with a minimal management structure.

DACTEC's M.D. will consider all such concerns expressed and will act to minimise any risks identified as he sees fit. In the event of a Breach of Data Protection he will respond in accordance with the procedures set out in this policy.

Because of the size of DACTEC Ltd no formal system or arrangement has been made for consultation with Customers, Suppliers or others in matters of Data Protection. All such matters should be discussed directly with the M.D. Employees of the Company will be proved with training to ensure adherence with GDPR.

Personal Data Audit (Collection)

The Personal Data that DACTEC Ltd collects and processes is as follows

- Personal contact details of Customers and Suppliers may include:
  1. Name
  2. Telephone numbers – Company landline + mobile
  3. Company Email addresses
- Employee Details:
  1. Personal contact details as above.

Personal Data Audit (Storage + Retention)

DACTEC Ltd stores the Personal Data records it has collected in the following manner:

All of these are stored on the DACTEC PCs and the M.D's mobile phone.
All of these devices are password protected and backed up securely.

Consent Policy

DACTEC Ltd shall seek appropriate valid consent from the Customers or Suppliers before any personal data is collected.

Consent for Data Protection Purposes

There are new and specific requirement with regard to consent when collecting and processing personal data. This data / information must be

- freely given,
- specific,
- informed
- unambiguous
- verifiable
- include a positive indication of agreement

A Customer, employee or Supplier has the right to withdraw consent for Data processing at any time and exercise of this right must be notified to DACTEC Ltd

The M.D of DACTEC Ltd- the Data Controller, will provide a form on which to record consent for data processing. This consent form will form part of the audit trail.

This policy applies to all employees working for DACTEC Ltd.

It is the responsibility of all employees to ensure that consent is obtained for all interactions.

Obtaining Consent

Consent is a Customer, employee or Supplier's agreement for DACTEC Ltd to collect their personal Data. This consent will be recorded on a consent form.

Anybody has the right to refuse consent for data collection, storage or processing. But this may make it impossible to carry out Support of our Customers.

Consent for Data Collection

Consent for Data Collection, Processing and Retention
DACTEC Ltd

DACTEC Ltd collects and uses personal data on the basis of your explicit consent having been given when you gave us your contact details, and in order to support your chamber needs. Your personal data will not be used for any other purpose.

Your data will be processed in a fair manner and retained by DACTEC Ltd for a period of 10 years after your last interaction with us. Your data will be stored securely and protected during this time.

Your data will not be subjected to automated processing by DACTEC Ltd.

You have a number of rights in relation to your personal data held by DACTEC Ltd. These include

a. the right to request from us access to and rectification or erasure of your personal data,
b. the right to restrict processing, object to processing as well as in certain circumstances the right to data portability
c. The right to withdraw your consent for the processing of your data (in certain circumstances) at any time which will not affect the lawfulness of the processing before your consent was withdrawn.
d. The right to lodge a complaint to the Data Commissioners Office if you believe that we have not complied with the requirements of the GDPR or DPA with regard to your personal data.

The Data Controller and the Data Protection Officer is the M.D.

Privacy Notice for Employees
Data Collection + Processing

Privacy Notice

How your information will be used

1. As your employer, DACTEC Ltd needs to keep and process information about you for normal employment purposes. The information we hold and process will be used for our management and administrative use only. We will keep and use it to enable us to run the business and manage our relationship with you effectively, lawfully and appropriately,
   - during the recruitment process,
   - whilst you are working for us,
   - at the time when your employment ends and after you have left

   This includes using information to enable us to comply with the employment contract, to comply with any legal requirements, pursue the legitimate interests of the Company and protect our legal position in the event of legal proceedings.
   If you do not provide this data, we may be unable in some circumstances to comply with our obligations and we will tell you about the implications of that decision.
2. As a Company pursuing business activities, we may sometimes need to process your data as a result of your employment contract or to pursue our legitimate business interests, for example to promote the your skills on our website. We will never process your data where these interests are overridden by your own interests.
3. Much of the information we hold will have been provided by you, but some may come from other sources, such as referees.
4. The sort of information we hold includes Used Hours lists, contact information, bank account and salary details.
5. Where we are processing data based on your consent, you have the right to withdraw that consent at any time.
6. Other than as mentioned below, we will only disclose information about you to third parties if we are legally obliged to do so or where we need to comply with our contractual duties to you, for instance we may need to pass on certain information to payroll provider, auditors, pension or health insurance schemes.
   In limited and necessary circumstances, your information may be transferred outside of the EU. We have in place safeguards to ensure the security of your data.
7. Your personal data will be stored for a period of 10 years following your employment ending.
8. If in the future we intend to process your personal data for a purpose other than that which it was collected we will provide you with information on that purpose and any other relevant information.
9. Your rights under the General Data Protection Regulation (GDPR) and The Data Protection Act (DPA) with regard to your personal data. You have
   a. the right to request from us access to and rectification or erasure of your personal data,

b. the right to restrict processing, object to processing as well as in certain circumstances the right to data portability
c. The right to withdraw consent if you have provided consent for the processing of your data (in certain circumstances) at any time which will not affect the lawfulness of the processing before your consent was withdrawn.
d. The right to lodge a complaint to the Data Commissioners Office if you believe that we have not complied with the requirements of the GDPR or DPA with regard to your personal data.

The Company CEO is the Data Controller and processor of data for the purposes of the DPA and GDPR.

If you have any concerns as to how your data is processed you can contact:

David Toner Tel: 0872370674 Email: contact@dactecltd.com
M.D & Data Protection Offer.

Access Request Policy

DACTEC Ltd will provide access to a full copy of the personal data which it holds on any individual on receipt of a written request for same. An informal request will be sufficient to begin the process of retrieval and copying of the data.

The data will be made available to the data subject on receipt of a written request. The written request must identify the data subject clearly and specify precisely what data of theirs the request applies to. The request in writing permits the company to maintain a clear audit of its records.

A copy of the data record will be provided in hard copy and either delivered by

1. Hand
2. Mail to a specific name and addressed person

The transfer of the data record needs to be documented and recorded itself to provide an audit trail.

Electronic copies can only be provided where it has been requested in this format and will be sent to a specified email address that is specific to a named recipient as set out in the original written request for the access / copy of the record. A 'read' or 'opened' or 'delivery' receipt will be requested from the email service provider in order to provide an audit trail.
Alternatively the data subject may provide a media device where the electronic record can be transferred and a written confirmation of receipt will be requested.

All email that includes personal data will be sent to specific named individuals email addresses.

Where a request is made to correct the data record the request to do so must specify exactly which data in the record is incorrect, and if possible indicate what change needs to be made in the record in order to correct it.

Where a conflict arises between the rights of the data subject and the data controller – DACTEC Ltd – the M.D. will make contact with the data subject and outline the nature of and implications of the conflict, in order to achieve a mutually agreeable solution. i.e. where the data subject may request deletion of a record but there is a legal requirement for the company to retain it.

Once the requested change or deletion of a record has been completed the Company will provide confirmation of having done so to the data subject.

Sharing Data / Transfer of Data Policy

DACTEC Ltd will not normally share your personal data with any other person or organisation. It is the policy of the Company to seek and receive your permission prior to doing so.

Your consent will be required to share any information about you with any other third party. Your consent will be sought and recorded in your personal record notes.

A written request will be required whether from you, the data subject, or from the third party themselves setting out clearly whom they wish information about, what information they require, when the require it, the purpose for which they require it and how it should be provided.
Any request from a third party will be checked with you, the data subject, before any information is shared.
A record of the request and the transfer of data will be made in the personal record record.

All personal data shared will be transferred to a specific individual either directly by hand, by mail to a specified person or by email to a specified personal email address. In the latter case the file may be password protected / encrypted and the password provided separately from the electronic file.

Records will be included in any sale of the company and should be considered as a transfer of ownership and thus needs to be recorded

This Company will not share retained personal data with third parties for advertising or marketing / promotion purposes.

Records Retention Policy

It is the policy of this Company to retain the Personal Data it has processed for a period of not less than 10 years from the last interaction with the data subject.

All retained records containing personal data will be stored safely, securely and in such a way as to preserve its privacy and confidentiality.

Access to personal data will be restricted to those who reasonably require it in order to perform their work within the Company.

Personal Data will not be shared with other persons other than by the expressed consent of the data subject.

Archived records older than ten years have been retained in case they were needed in the past. It is the policy of the Company to gradually begin reviewing these records and where no reason is found to retain them they will be destroyed or anonymised.

Records will be reviewed on an annual basis. Records that are older than 10 years, that have no apparent reason for retaining them longer, will be deleted.

Records that are held beyond this period where possible will be anonymised. Where a record is retained and cannot be anonymised an explanation will be provided to the data subject and a further consent to retain the record will be sought.

Destruction of the records will be arranged in such a way as to ensure the safety and confidentiality of the data.

This company will not share retained personal data with third parties for advertising or marketing / promotion purposes.

Data Storage Policy

Paper records

Employment and other HR Records are kept on password protected computers.

Electronic / Digital Records

The standard of encryption required to adequately secure data changes with advances in technology. Whole-disk encryption of 256-bit strength should meet the requirement at present and is provided by the current PC.

The company computer / PC is protected by a password

The PC is provided with antivirus protection that provides daily updates and up to the minute protection for internet security.

The WIFI internet used within the company is password protected.

Other Data

The premises are protected by an alarm system when the company is not in use.

Registration Details
Data Protection Commissioners

Complete the details of your business registration details with the DPC here

Reporting Data Breaches

Once detected all data breaches will be reported directly on the DPC website at the following link which provides detailed information on dealing with breaches.

More information is available at the following webpage data security breach Code of Practice

The Breach will be reported to the following contact options.

1. E-Mail - dpcbreaches@dataprotection.ie
2. Phone - 1890 252231(lo-call); 00 353 (0) 57 8684800
3. Fax- 00 353 (0) 57 8684757

Housekeeping / Good Operational Practice

All information that may identify an individual is considered personal data. Therefore the concept of good housekeeping practice is inherent in keeping personal information private and confidential.

All phone conversations should be conducted in a manner to maximise privacy of the persons involved. Use of names and phone numbers in public areas in association with other business details should be avoided.

Careful use of PCs will allow Customer data to be kept safe and confidential. The PC is provided with appropriate levels of software protection, anti -virus protection etc.

Email + Electronic Communication

Sending E-mails

1. Before sending a message check the addresses.
2. Identify yourself in each message, include your name at the end of a message.
3. Use subject headers or titles that will have meaning for the recipient
4. Copy relevant individuals and indicate in the message who is receiving copies.
5. If you are going to be unavailable on e-mail, leave a message to that effect or make alternative arrangements
6. E-mail messages are part of the formal communication for the company as a whole and therefore should reflect a professional manner and tone.
7. Aim to respond to emails received when required within a reasonable time frame. Send a response indicating where this is not possible and when a response may be expected.

Content

1. Use the subject field to indicate clearly what the content is about.
2. Avoid writing in CAPITAL LETTERS as this is the electronic version of shouting.
3. Keep humour appropriate – it can often be misinterpreted.
4. Avoid sending unnecessary information – keep e-mails brief and to the point

Attachments

1. Careful consideration should be given before sending attachments, Attachments should always be sent as a common file type e.g. PDF, Word, Excel etc.
2. The sender should clearly state on the email what the attachment is and the purpose for sending it, to minimise the spread of viruses.

Sensitive Information

1. Be professional - e-mail is easily forwarded.
2. Be aware of copyright and libel issues.
3. It is not the policy of DACTEC Ltd to send emails that are offensive, threatening, defamatory or illegal.

Receiving E-Mails

1. E-mails should be read by the intended recipient only.
2. E-mail accounts should be accessed on a regular basis at least once per day.

Detecting + Reporting of Breaches

The responsibility for all data protection lies with DACTEC Ltd, the M.D and Data Protection Oficer.

As the person responsible for all aspects of Data Protection, he is also responsible for Detection of and reporting of Breaches of Data security.

Under GDPR requirements on detection of a data breach DACTEC Ltd will report the breach to the DPC 72 hours, unless the data was anonymised or encrypted.

It is the policy of this company to inform the individual(s) impacted by the breach and to keep them informed of progress of investigations + remedial actions taken.

If a data breach is discovered immediate action will be taken to minimise any further loss of data or unauthorised access to the data.

Disconnect the PC and other devices from the internet. Disconnect the internet modem from the phone line

Determine the extent of the breach and what data is affected / has been compromised and whose data it is.

Determine who has perpetrated the breach and how. Take steps or advice on how to close the breach and prevent further exploitation of this security weakness.

Prepare a report for the DPC and submit it within 72 hours or sooner if possible.

Anyone acting suspiciously or apparently trying to gain access to data is warned that this is unacceptable behaviour. Failure to correct such behaviour or persistence with it will result in their exclusion from the premises.

Specialist guidance will be sought from the website hosting company about apparent irregularities. The company website has information for public consumption but no direct personal data is collected or stored in any database as part of the website.

Data Protection Risk Assessment

No	Data Hazard / Risk	Risk Level	Control Measure
1	Website being hacked	Med	Have suitable protection in place by Hosting Service. Provide protection for website databases where present
2	Unauthorised access to PC	High	Use password protection for Starting PC Password protection for all users of company software systems
3	Screens visible by visitors	Low	PC is positioned in our office which is nor accessed by any non-employees. We use a screen auto-logoff. Laptop access is similarly controlled.
8	Contractors working in premises unsupervised	Medium	Lock PC screen if unsupervised
11	Phone conversations being overheard	High	Keep phone conversations where sensitive data likely to be discussed to a minimum until alone.
12	Robbery / theft / unauthorised entry to the premises	High	Always lock thePC