

# FarmLab Diagnostics General Data Protection Regulation (GDPR) Policy

## Introduction

Background to the General Data Protection Regulation (GDPR)

The GDPR 2016 replaces the EU Data protection Directive of 1995 and supersedes the laws of individual member states that were developed in compliance with the Data Protection Directive 95/46/EC. Its purpose is to protect the “rights and freedoms” of natural persons (i.e. living individuals) and to ensure that personal data is not processed without their knowledge, and, wherever possible, that it is processed with their consent.

As part of our normal everyday operations, the FarmLab Diagnostics 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 is collected, handled and stored to meet the company’s data protection standards and to comply with the applicable law(s).

It is important to point out that we may amend this Privacy Policy from time to time.

## Definitions

Personal Data: any information relating to an identified or identifiable natural person (data subject); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as name, an identification number, location data, an online identifier or to one or more factors specific to the physical, genetic, mental, economic, cultural or social identity of that natural person.

Special categories of personal data: personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of genetic data,

biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

#### Purpose of this Policy

This data privacy policy ensures FarmLab Diagnostics :

Complies with data protection law and follows best practise,

Protects the rights of staff, customers and partners,

Is open and transparent about how it processes and stores individual's data,

Protects itself from the risks of a data breach.

#### Data Protection Law

The Data protection acts 1998 and 2003 describe how organisations 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 data must:

Be processed fairly and lawfully,

Be obtained only for specific, lawful purposes,

Be adequate, relevant and not excessive,

Be accurate and kept up to date,

Not be held for any longer than necessary,

Processed in accordance with the rights of data subjects,

Be protected in appropriate ways,

Not be transferred outside the European Economic Area (EEA), unless that country or territory also ensures an adequate level of protection.

## **PEOPLE, RISKS AND RESPONSIBILITIES**

Policy Scope

This policy applies to:

All staff of FarmLab Diagnostics

All contractors, suppliers and other parties working on behalf of FarmLab Diagnostics

It applies to all data that the organisation holds relating to identifiable individuals, even if that information falls outside of the Data Protection Acts 1998 and 2003. This data can include:

Full names of individuals,

Postal addresses,

Personal e-mail addresses including individuals full names,

Telephone numbers,

Author: John Gilmore

Approved by: Marese Cregg

Approval date: 25/11/2019

Page 3 of 16

Status: Current

plus any other information relating to individuals.

#### Data Protection Risks

This policy has been put in place to offer our customers full transparency while also helping to protect FarmLab Diagnostics from data security risks, including,

Breaches of confidentiality such as information been given out inappropriately or accidentally,

Failing to offer choice e.g. all individuals should be free to choose how the company uses data relating to them,

Reputational damage the company could suffer should hackers successfully gain access to sensitive data.

#### Responsibilities

Everyone who works for FarmLab Diagnostics 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, the board of directors is ultimately responsible for ensuring that FarmLab Diagnostics meets its legal obligations.

#### GENERAL STAFF GUIDELINES

The only people able to access data covered by this policy should be those who need it to conduct their work.

Data should not be shared informally. When access to confidential information is required, employees can request it from their line managers.

FarmLab Diagnostics 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 manager or the Data Protection Officer if they are unsure about any aspect of data protection.

#### **HOW DO WE COLLECT PERSONAL DATA?**

We collect personal data in two primary ways:

Personal data that you the Employee, Customer, Supplier or Job Applicant proactively gives to us i.e. name, address, e-mail address, CVs etc.

Personal data that we receive from other sources such as websites, colleagues, referees etc.

#### **Categories of individuals / entities who provide data to FarmLab Diagnostics**

**Customer** – to ensure that we provide you with the best service possible, we store your personal data and/or the personal data of individual contacts at your organisation as well as keeping records of our conversations, meetings, registered jobs and placements. From time to time, we may also ask you to undertake a customer satisfaction survey. We think this is reasonable – we deem these uses of your data to be necessary for our legitimate interests as an organisation providing various recruitment services to you.

**Suppliers**– we use and store the personal data of individuals within your organisation in order to facilitate the receipt of services from you as one of our Suppliers. We also hold your financial details, so that we can pay you for your services. We deem all such activities to be necessary within the range of our legitimate interests as a recipient of your services.

**Job applicant** – completed job applications or CVs for the purposes of gaining employment with FarmLab Diagnostics.

Personal data we receive from other sources -

We also receive personal data about Customers, Suppliers or Job Applicants from other sources. Depending on the relevant circumstances and applicable local laws and requirements, these may include personal data received in the following situations:

Your CV referees may disclose personal information about you;

We may obtain information about you from searching third party sources, such as LinkedIn and other job sites;

Our other Customers or Suppliers may share personal information about you or your organisation with us.

Website users:

Visitors are advised that each time they visit the Farmlab Diagnostic's website , two general levels of information about their visit can be retained.

The first level comprises statistical and other analytical information collected on an aggregate and non-individual specific basis of all browsers who visit the site. The second is information which is personal or particular to a specific visitor who knowingly chooses to provide that information.

The statistical and analytical information provides general and not individually specific information about the number of people who visit this Website; the number of people who return to this site; the pages that they visit; where they were before they came to this site and the page in the site at which they exited. This information helps us monitor traffic on our Website so that we can manage the site's capacity and efficiency. It also helps us to understand which parts of this site are most popular and generally to assess user behaviour and characteristics in order to measure interest in and use of the various areas of the site.

Through this Website you may have an opportunity to send us information, such as through the "registration" pages or any other area where you may send e-mails, provide feedback, etc. By choosing to participate in these, you will be providing us with some level of personal information relating to you. This information will only be used by this site for:

the purposes for which it was provided by you;  
verification purposes and statistical analysis; and  
marketing and administration purposes.

The website does not collect any personal data about you apart from information which you volunteer (for example, by emailing us, or registering with us). Any information which you provide in this way is not made available to any third parties and is used by this site only in line with the purpose for which you provided it.

#### DATA STORAGE

How do we safeguard your personal data?

We are committed to taking all reasonable and appropriate steps to protect the personal information that we hold from misuse, loss, or unauthorised access. We do this by having in place a range of appropriate technical and organisational measures. These include measures to deal with any suspected data breach.

If you suspect any misuse or loss of or unauthorised access to your personal information please let us know immediately. Details of how to contact us can be found at the end of this policy.

How long do we keep your personal data for?

FarmLab Diagnostics retains your Personal Information for the period necessary to fulfill the purposes outlined in this Privacy Policy, unless a longer retention period is required by law or to fulfill a legal obligation.

We continuously assess and delete data to ensure it not held for longer than necessary.

Laboratory test related data HCSI will be retained for a period up to and including 7 years. All data will be handled through normal security mechanisms to ensure that access is restricted.

## Storage and transfer of data

In order to provide you with the best service and to carry out the purposes described in this Privacy Policy, your data may be transferred:

to an approved and nominated third party data storage facility,

to an approved and nominated cloud-based storage/ software provider.

We want to make sure that your data are stored and transferred in a way which is secure. We will therefore only transfer data outside of the European Economic Area or EEA (i.e. the Member States of the European Union, together with Norway, Iceland and Liechtenstein) where it is compliant with data protection legislation and the means of transfer provides adequate safeguards in relation to your data, for example:

by way of data transfer agreement, incorporating the current standard contractual clauses adopted by the European Commission for the transfer of personal data by data controllers in the EEA to data controllers and processors in jurisdictions without adequate data protection laws; or

transferring your data to a country where there has been a finding of adequacy by the European Commission in respect of that country's levels of data protection via its legislation; or where it is necessary for the conclusion or performance of a contract between ourselves and a third party and the transfer is in your interests for the purposes of that contract (for example, if we need to transfer data outside the EEA in order to meet our obligations under that contract if you are a Client of ours); or where you have consented to the data transfer.

To ensure that your personal information receives an adequate level of protection, we have put in place appropriate control measures with our approved third party suppliers who may have access to your personal data with to ensure that your personal information is treated by those third parties in a way that is consistent with and which respects the law on data protection.

## CONSENT

In certain circumstances, we are required to obtain your consent for the processing of your personal data in relation to certain activities. Depending on exactly what we are doing with your information, this consent will be opt-in consent or soft opt-in consent.



Article 4(11) of the GDPR states that (opt-in) consent is "any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her." In plain language, this means that:

- You have to give us your consent freely, without us putting you under any type of pressure,
- You have to know what you are consenting to – so we'll make sure we give you enough information,
- You should have control over which processing activities you consent to and which you don't,
- you need to take positive and affirmative action in giving us your consent – we're likely to provide a tick box for you to check so that this requirement is met in a clear and unambiguous fashion.

We will keep records of the consents that you have given in this way.

Marketing - We have already mentioned that, in some cases, we will be able to rely on soft opt-in consent. We are allowed to market products or services to you which are related to the products or services we provide as long as you do not actively opt-out from these communications.

Right to withdraw consent:

Where we have obtained your consent to process your personal data for certain activities, you may withdraw this consent at any time and we will cease to carry out the particular activity that you previously consented to unless we consider that there is an alternative reason to justify our continued processing of your data for this purpose in which case we will inform you of this condition.

## DATA USE

Personal data is of no value to the farmlab Diagnostics 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 private 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.

What are the lawful bases for processing?

Legitimate interests:

Article 6(1)(f) of the GDPR states that we can process your data where it "is necessary for the purposes of the legitimate interests pursued by [us] or by a third party, except where such interests are overridden by the interests or fundamental rights or freedoms of [you] which require protection of personal data."

The lawful bases for processing are set out in Article 6 of the GDPR. At least one of these must apply whenever you process personal data:

- a) Consent: the individual has given clear consent for you to process their personal data for a specific purpose,
- b) Contract: the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract,
- c) Legal obligation: the processing is necessary for you to comply with the law (not including contractual obligations),
- d) Vital interests: the processing is necessary to protect someone's life,
- e) Public task: the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law,
- f) Legitimate interests: the processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which

overrides those legitimate interests. (This cannot apply if you are a public authority processing data to perform your official tasks.)

Who do we share your personal data with?

Where appropriate and in accordance with local laws and requirements, we may share your personal data, in various ways and for various reasons, with the following categories of people:

Animal Health Ireland or the Irish cattle Breeders federation, or other third party with whom you have given your consent for us to transfer data.

Department of Agriculture Food and the Marine, where there is a regulatory requirement for us to do so under Notifiable Disease regulations or other relevant statutory regulations/ legislation

Tax, audit, or other authorities, when we believe in good faith that the law or other regulation requires us to share this data (for example, because of a request by a tax authority or in connection with any anticipated litigation);

Third party service providers who perform functions on our behalf such as lawyers, auditors and accountants, technical support functions and IT consultants carrying out testing and development work on our business technology systems;

Third party outsourced IT and document storage providers where we have an appropriate processing agreement (or similar protections) in place;

## DATA ACCURACY

The law requires that the FarmLab Diagnostics 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 FarmLab Diagnostics should put into ensuring its accuracy.

It is the responsibility of all employees who work with data to take reasonable steps to ensure personal data 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.

Data should be updated as inaccuracies are discovered.

#### DATA SUBJECT ACCESS REQUESTS

You have various rights relating to how your personal data is used including the right:

To ask for access to the information we hold on you;

To change information you think is inaccurate;

To delete information (your right to erasure); Subject to regulatory requirements in relation to data storage

To ask us to limit what we use your data for;

To have your personal data moved to another IT environment in a safe and secure way, without affecting its usability. (data portability);

To make a complaint.

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

You may ask us to confirm what information we hold about you at any time, and request us to modify, update or delete such information. We may ask you to verify your identity and for more information about your request. If we provide you with access to the information we hold about you, we will not charge you for this unless your request is "manifestly unfounded or excessive". If you request further copies of this information from us, we may charge you a reasonable administrative cost where legally permissible. Where we are legally permitted to do so, we may refuse your request. If we refuse your request we will always tell you the reasons for doing so. The data controller will aim to provide the relevant data within 30 days.

All individuals who are the subject of personal data held by FarmLab Diagnostics 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.

Subject access requests from individuals should be made by email, addressed to the data controller at [info@farmlab.ie](mailto:info@farmlab.ie) with "Data protection" in subject line . The data controller can supply a standard request form, although individuals do not have to use this.

Right to erasure:

You have the right to request that we erase your personal data in certain circumstances. Normally, the information must meet one of the following criteria:

the data is no longer necessary for the purpose for which we originally collected and/or processed it;

where previously given, you have withdrawn your consent to us processing your data, and there is no other valid reason for us to continue processing;

the data has been processed unlawfully (i.e. in a manner which does not comply with the GDPR);

it is necessary for the data to be erased in order for us to comply with our legal obligations as a data controller; or

if we process the data because we believe it necessary to do so for our legitimate interests, you object to the processing and we are unable to demonstrate overriding legitimate grounds for our continued processing.

Please note that we comply with local law requirements regarding data subject right to erasure and may refuse your request in accordance with local laws.

We would only be entitled to refuse to comply with your request for one of the following reasons:

to exercise the right of freedom of expression and information;

to comply with legal obligations or for the performance of a public interest task or exercise of official authority;

for public health reasons in the public interest;

for archival, research or statistical purposes; or

to exercise or defend a legal claim.

When complying with a valid request for the erasure of data we will take all reasonably practicable steps to delete the relevant data.

Data destruction – while we will endeavour to permanently erase your personal data once it reaches the end of its retention period or where we receive a valid request from you to do so, some of your data may still exist within our systems, for example if it is waiting to be overwritten. For our purposes, this data has been put beyond use, meaning that, while it still exists on an archive system, this cannot be readily accessed by any of our operational systems, processes or Staff.

### **CROSS BORDER DATA TRANSFERS**

We may share personal data outside the EU, however we will always ensure that this is done in compliance with the relevant laws.

We ensure that any transfer of data outside the EU is undertaken using legally compliant transfer mechanisms and in accordance with the GDPR.

When we transfer personal data outside of the EU, we generally rely on the Standard Contractual Clauses under Article 46.2 of the GDPR adopted by the EU Commission however we may also rely on some of the other legally compliant transfer mechanisms.

### **DISCLOSING DATA FOR OTHER REASONS**

In certain circumstances, the General Data Protection Regulation allows personal data to be disclosed to law enforcement agencies without the consent of the data subject.

Under these circumstances, FarmLab Diagnostics 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**

Author: John Gilmore

Approved by: Marese Cregg

Approval date: 25/11/2019

Page 14 of 16

Status: Current

Key information:

FarmLab Diagnostics Data Protection Officer/ Data Controller: info@farmlab.ie

Policy prepared by: John Gilmore, Data protection officer

How to contact your local supervisory authority

Details of your local supervisory authority:

The Office of the Data Protection Commissioner. They can be contacted in the following ways:

Phone: (+353;) 57 8684800 or (+353) (0)761 104 80 or 1890 252 231 (Local)

Email: info@dataprotection.ie

Post: - Dublin Office: 21 Fitzwilliam Square, Dublin 2, D02 RD28, Ireland

Portarlinton Office (Postal Address): Canal House, Station Road,  
AP23, County Laois, Ireland

Portarlinton, R32

Fax: (+353) 57 868 4757.

Collection and use of non-personal information

Non-personal information: data collected for statistical purposes which is not associated with a specific identity. This site collects and analyses technical information in order to evaluate our Website. The type of technical information we log is confined to the following:

The IP address\*1 of the visitor's Web server

The top-level domain-name used (for example .ie, .com, .org, .net)

The pages visited on our Website, i.e. URL's\*2 visited

The previous Website address from which the visitor reached us, including any search terms used

Clickstream data which shows the traffic of visitors around this Website (for example, pages accessed)

\* An IP address is an identifier for a computer or device on a Transmission Control Protocol/Internet Protocol (TCP/IP) network, such as the World Wide Web. Networks use the TCP/IP protocol to route information based on the IP address of the destination. In other words, an IP address is a number that is automatically assigned to your computer whenever you are surfing the Web, allowing Web servers to locate and identify your computer. Computers require IP addresses in order for users to communicate on the Internet, browse and shop.

\*2 A URL (Uniform Resource Locator) is the global address of documents and other resources on the World Wide Web.