Data Protection Policy

1. Introduction

LMIS Global (Europe) B.V. (LMIS) 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 organisation's data protection standards — and to comply with the law.

2. Purpose

The principles underlying this data protection policy ensures that LMIS

- Complies with Data Protection legislation 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 or cyber-attack on its systems.

3. Scope

3.1. This policy applies to all personal data and special categories of personal data (previously known as sensitive data) processed by LMIS and as defined under the General Data Protection Regulation (GDPR) / AVG in Dutch, including structured sets of personal data held in electronic or other filing systems that are accessible according to specified criteria.

3.2. 'Personal Data' means any information relating to an identified or identifiable living individual. Identifiable living individual means a living individual who can be identified, directly or indirectly, in particular by reference to:

a) an identified such as a name, an identification number, location data or an online identified; or
b) one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of the individual.

3.3. This can include:

- Names of individuals.

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

3.4. For personal data to be processed lawfully, one or more of the following legal grounds must apply:

- The data subject has given consent to the processing of their personal data for one or more specific purposes.
- 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.
- Processing is necessary for compliance with a legal/statutory obligation to which the controller is subject to.
- Processing is necessary in order to protect the vital interests of the data subject or of another natural person.
- 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 controller.
- Processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party.

Special categories of personal data (sensitive data)

3.5. These are personal data deemed to be more sensitive by law, and so need additional protection. They cannot be processed unless at least one further condition for processing special category data is fulfilled. These conditions are:

- The data subject has given explicit consent:
- The processing is necessary in the context of employment law, or laws relating to social security and social protection.
- The processing is necessary to protect vital interests of the data subject or of another natural person.
- The processing is carried out in the course of the legitimate activities of the company, with respect to its own members, former members, or persons with whom it has regular contact in connection with its purposes.
- The processing relates to personal data which have been manifestly made public by the data subject.
- The processing is necessary for the establishment, exercise or defence of legal claims, or for courts acting in their judicial capacity.

- The processing is necessary for reasons of substantial public interest, and occurs on the basis of a law that is, inter alia, proportionate to the aim pursued and protects the rights of data subjects.
- The processing is necessary for archiving purposes in the public interest, for historical, scientific, research or statistical purposes, subject to appropriate safeguards.

4. The Policy

4.1. This Policy sets out our commitment to protecting personal data; how this commitment is implemented with regard to the collection and use of personal data; and ensuring the rights of individuals whose data is held (the Data Subject) can be exercised as prescribed by the General Data Protection Regulation. We are committed to ensuring that it complies with the underpinning six data protection principles, as listed below.

4.2. The 6 Data Protection Principles:

- Personal data shall be processed lawfully, fairly and in a transparent manner in relation to individuals;
- Personal data shall be obtained for one or more specified, explicit and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes;
- Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
- Personal data shall be accurate and, where necessary, kept up to date;
- Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed;
- Personal data shall be 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.

4.3. These principles will be adhered to with the following ambitions:

- Meeting our legal obligations as laid down by the GDPR;
- Ensuring that data is collected and used fairly, lawfully and transparently;
- Processing personal data where an appropriate legal basis to do so exists and only in order to meet our operational needs or fulfil legal requirements;
- Taking steps to ensure that personal data is up to date and accurate;

- Establishing appropriate retention periods for personal data (see our Privacy Statement for more information);
- Ensuring that data subjects' rights can be appropriately exercised;
- Ensuring that a nominated officer is responsible for data protection compliance and provides a point of contact for all data protection issues, i.e. Data Protection Officer;
- Ensuring that all staff are made aware of good practice in data protection (all staff are required to sign a GDPR Confidentiality Agreement);
- Providing adequate training for all staff responsible for personal data;
- Ensuring that everyone handling personal data knows where to find further guidance;
- Ensuring that queries about data protection, internal and external to the organisation, are dealt with effectively and promptly;
- Sharing information where required by law and where approved information sharing agreements are in place and when agreed processes have been followed;
- Regularly reviewing data protection procedures and guidelines within the organisation;
- Adopting local and EU data protection best practice, including incorporation of appropriate learning from any published European Data Protection Board (EDPB) guidance;
- Publishing and promoting this policy and the rights of data subjects including how to make a right of access request;
- Registering with the European Data Protection Board as an organisation which handles data;
- Establishing procedures for reporting data protection breaches to relevant authorities for investigation, including self-referral mechanisms;
- Being clear with individuals whose data we process as to how we store it, what we do with it and why (see Privacy Statement);
- Responding to any valid subject access requests promptly and in any event within one month of receiving them (unless limited exceptions apply).

4.4. This Policy helps to protect us from some very real data security risks, including:

- Breach of confidentiality and public trust; for instance, information being shared inappropriately;
- Failing to offer choice; for instance, all individuals should be free to choose how the organisation uses data relating to them when the processing is by consent;
- Failing to observe the enhanced rights that citizens have under the GDPR - for example, right of access, right to rectification, etc;

- Reputational damage: for instance, LMIS could suffer if hackers were to successfully corrupt, gain access to or steal sensitive data.

5. Data Protection Risks

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

- Breach of confidentiality and public trust; for instance, information being shared inappropriately.
- Failing to offer choice; for instance, all individuals should be free to choose how the organisation uses data relating to them when the processing is by consent.
- Failing to observe the enhanced rights that citizens have under Data Protection Legislation GDPR – for example, right of access, right to rectification, etc.
- Reputational damage; for instance, LMIS could suffer if hackers were to successfully corrupt, gain access to or steal sensitive data.

6. Roles and Responsibilities

6.1. LMIS's responsibilities:

- LMIS is the data controller under Data Protection Legislation for the personal data it processes for its own purposes:
- The Data Protection Officer (DPO) has overall responsibilities for compliance with Data Protection legislation;
- The DPO is responsible for monitoring progress and advising the organisation on implementation of this policy; acting as primary contact on any data protection queries; and approving responses to Right of Access requests (generally described in this document as 'Subject Access Requests');
- The DPO is also responsible for monitoring the completion of all mandatory training for all staff (with special emphasis on staff handling personal data on daily basis) and to ensure access to further guidance and support;
- LMIS provides clear lines of reporting and an appropriate separation of duties to allow the DPO to supervise compliance with GDPR, reporting to board level;
- The DPO will conduct regular assurance activity to monitor and assess new processing of personal data;
- The DPO will monitor and report on all data processor requirements e.g. Roles & Responsibilities, notification, data subject access requests;

- The DPO is the first point of contact for the regulatory authorities and for individuals whose data is processed (employees, customers etc.).

6.2. Employee Responsibilities.

- All employees have individual responsibility for complying with this Policy and following accompanying guidance.
- All employees will undertake relevant data protection training, and any other training that shall be deemed as mandatory.

6.3. Employees will:

- Observe all forms of guidance, codes of practice and procedures about the collection, sharing, handling and use of personal information;
- Develop a comprehensive understanding of the purpose for which LMIS uses personal information;
- Collect and process information in accordance with the purpose for which it is required to be used by LMIS to meet its statutory requirements and business needs;
- Ensure the information is destroyed when no longer required in line with our information management guidance;
- Upon receipt of a request by or on behalf of an individual for information held about them (Subject Access Request), staff will refer requests to the DPO as quickly as possible so that the request can be acted on quickly and legal advice sought if required.
- Understand that breaches of this policy may result in scrutiny by the European Data Protection Board (EDPB) with the potential for fines to be levied and accompanying reputational damage. There is also the potential for misconduct action.

7. Data Protection Impact Assessments

7.1. A Data Protection Impact Assessment (DPIA) will be carried out if a project or the introduction of a new service or policy is likely to result in a high risk to the privacy of individuals. A DPIA is a process that helps identify privacy risks and ensure lawful practice when a new project is designed, or changes are made to an existing service or policy.

7.2. The purpose of the DPIA is to ensure that privacy risks are mitigated including promptly addressing any identified issue while allowing the aims of the project or policy to be met whenever possible.

7.3. Good practice would dictate that a DPIA is required when an organisation plans to:

- Embark on a new project involving the use of personal data;
- Introduce new IT systems for storing and accessing personal information;
- Participate in a new data-sharing initiative with other organisations;
- Use profiling or special category data to decide on access to services;
- Initiate actions based on a policy of identifying particular demographics;
- Use existing data for a new and unexpected or more intrusive purpose;
- Match data or combine datasets from different sources;
- Collect personal data from a source other than the individual without providing them with a privacy notice ('invisible processing');
- Profile children or target services at them; or
- Process data that might endanger the individual's physical health or safety in the event of a security breach;
- Continue to utilise long standing databases where the DPIA may not have been considered previously or the legal or organisational framework has changed and may give rise to new privacy risks or issues.

7.4. Guidance issued by the European Data Protection Board can be found here:- https://edpb.europa.eu/edpb_en

8. Data Protection by Design and Default

8.1. In compliance with data protection by design principle, we will ensure data protection risks are taken into account throughout the process of designing a new process, product, policy or services, rather than treating it as an afterthought. This means assessing carefully and implementing appropriate technical and organisational measures and procedures from the outset to ensure the processing complies with the law and protects the rights of the data subjects.

8.2. To comply with data protection by design and by default principles, we will ensure mechanisms are in place within the organisation to ensure that, by default, only personal data which are necessary for each specific purpose are processed. This obligation includes ensuring that only the minimum amount of personal data is collected and processed for a specific purpose; the extent of processing is limited to that necessary for each purpose; the data is stored no longer than necessary, and access is restricted to that necessary for each purpose.

8.3. As with all risks posed by external actors, the likelihood that a ransomware attack is successful can be drastically reduced by tightening the security of the data controlling environment. The majority of IT breaches can be prevented by ensuring

that appropriate organizational, physical and technological security measures have been taken. Examples of such measures are proper patch management and the use of an appropriate anti-malware detection system. Having a proper and separate backup will help to mitigate the consequences of a successful attack should it occur. A proper patch management that ensures that the systems are up to date and all known vulnerabilities of the deployed systems are fixed is one of the most important since most of the ransomware attacks exploit well-known vulnerabilities.

9. Breach Notification and Reporting

9.1. GDPR defines a personal data breach in Article 4(12) as "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". A breach should be notified when the Controller is of the opinion that it is likely to result in a risk to the rights and freedoms of the data subject. Controllers should make this assessment at the time they become aware of the breach. The controller should not wait for a detailed forensic examination and (early) mitigation steps before assessing whether or not the data breach is likely to result in a risk and thus should be notified.

9.2. We must report any losses or suspected breaches of personal data to the Dutch Data Protection Authority using the data leak reporting desk https://datalekken.autoriteitpersoonsgegevens.nl/ (meldloket datalkeen) within 72 hours of becoming aware of the breach.

9.3. When the personal data breach is likely to result in a high risk to the rights and freedoms of individuals, we are required by law to notify the affected individuals without undue delay. If the data breach has led to unwarranted use of the data, that is, a cybercrime, you also need to report it to the Police.

9.4. If you discover or suspect a breach of data protection rule, loss or compromising of personal data, you must report it immediately to the Dutch Data Protection Authority (AP).

10. General Staff Guidelines

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

10.2. Personal data should not be shared without adherence to relevant guidance. When access to confidential information is required, employees can request it from their line managers.

10.3. LMIS will provide training to all employees to help them understand their responsibilities when handling data.

10.4. Employees should keep all data secure, by taking sensible precautions and following the guidelines below.

10.5. Strong passwords must be used, and they should never be shared.

10.6. Personal data should, under no circumstances, be disclosed to unauthorised individuals, either within the department or externally.

10.7. 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.

10.8. Employees should request help from their line manager or the Data Protection Officer if they are unsure about any aspect of Data Protection.

11. Data Storage

11.1. This Policy document describes how and where data should be safely stored. When data is stored on paper, it should be kept in a secure place where unauthorised people cannot see/access it.

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

- When not required, sensitive paper or files should be kept in a locked drawer or filing cabinet;
- Employees should make sure sensitive paper and printouts are not left where unauthorised people could see them, for example on a printer or unattended on a desktop:
- Sensitive data printouts should be shredded and disposed of securely when no longer required;

11.3. 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.
- If data is stored on removable media (e.g., data sticks), 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 service.
- 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 regularly tested.
- LMIS Data should under no circumstances be saved directly to personal laptops or other mobile devices such as tablets or smart phones.
- All servers and computers containing data should be adequately protected in line with GDPR/AVG/EDPB principles and standards.

12. Data Use

12.1. Personal data is of no value to LMIS 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 their computers are always locked when left unattended;
- Personal data should not be shared informally. In particular, it should never be sent by non-compliant webmail, as this form of communication is not secure;
- Personal data must be encrypted before being transferred electronically outside of those email domains approved within LMIS;
- Personal data should not be transferred outside of the European Economic Area except where appropriate safeguards have been put in place or the country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data;
- Employees should under no circumstances save copies of personal data to their own computers. Such data should always be accessed and updated via approved IT equipment.

13. Data Accuracy

13.1. The law requires LMIS to take reasonable steps to ensure data is kept accurate and up to date. It is incumbent upon LMIS to ensure personal data held and processed is

accurate and to ensure it continues to be accurate. 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.

13.2. Data will be held in as few places as necessary. Staff should not create any unnecessary additional data sets.

13.3. Staff should take every opportunity to ensure data is updated. For instance, by confirming a customer's details when they call.

13.4. LMIS will make it easy for data subjects to update the information it holds about them.

13.5. 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.

13.6. Where additional data sets are required the DPO should be engaged to ensure this is reflected on the LMIS Information Asset Register.

14. Right of Access Request / Subject Access Request

14.1. All individuals who are the subject of personal data held by LMIS are entitled to:

- Ask what information the organisation holds about them, how it is used and why'
- Ask how to gain access to it;
- Be informed how to keep it up to date;
- Be informed how the organisation is meeting its data protection obligations.

14.2. A request for access to personal information held by LMIS (known as Right of Access Request or a Subject Access Request) must be responded to within one calendar month.

15. Providing Information

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

- How the data is being used;
- Who it is shared with;

- How long it is kept for;
- How to exercise their rights.

15.2. To these ends, LMIS has a Privacy Statement, setting out how data relating to individuals is used by the organisation.

16. Monitoring, Review and Evaluation

16.1. The management will monitor the approach to data protection and associated rights.

16.2. This Policy will be reconsidered against any legislative changes and reviewed on an annual basis.

17. References, Legislation and Guidance

- The General Data Protection Regulation (AVG), 2016
- European Data Protection Board
- Dutch Data Protection Authority
- Dutch Government Information https://business.gov.nl/regulation/protection-personal-data/
- LMIS Privacy Statement
- LMIS Service Guide
- LMIS General Terms & Conditions.

Data Breach/Incident Reporting Form

Breach Reference:		
Date of incident:		
Time of incident:		
Location of incident:		
Person reporting incident:		
	Contact details:	
Name of company/person impacted:		
Details of incident:		
Was a 3rd party involved?		
Type of breach involved and sensitivity:		
	Is there a breach of confidentiality and has personal data been unintentionally disclosed?	
	Is it a breach of integrity and has the data been changed?	
	Is it a breach of availability and is the data no longer accessible?	
	If yes, number of individuals or records that may be at risk?	
	Is there potential for financial harm?	
What data has potentially been leaked/lost?		
	Estimate of whether the data leak poses a risk to	

	the rights and freedoms of the data subjects? *	
	*If there is no risk, you do not have to report the data breach to the data subjects. Do not underestimated these risks. Even innocent personal data can be extremely valuable in the wrong hands.	
	Has the individual concerned / data subject been informed?	
	Has a decision been taken not to inform? If so, why?	
	Has this not yet been decided? The DPO should be asked for advice before the individuals concerned are informed.	
Does any potentially impacted data come from a government-affiliated or public-sector entity, or from their contractors/sub-contractors?		
What incident management procedures or mitigation steps have been followed:		
What disciplinary action will be invoked?		
Full description of what happened (including whether it was a theft):		
	Accidental loss?	
	Inappropriate disclosure?	
	Procedural failure?	
	Unauthorised disclosure?	
How was the information held?	Paper/memory stick/laptop/ tablet or smart phone etc?	
	If digital format, was it encrypted? Is the key still secure? *	
	* If the personal data is encrypted and the key is still secure, then it does not have to be reported, unless access to the data has been lost by LMIS. If that is	

	the case, then this is classed as a breach of availability.	
Is there potential for media interest?		
Are there any legal implications?		
Who has been informed within LMIS?		
Have the IT team been informed?		
Has an online report been submitted to the Dutch Data Protection Authority? https://datalekken.autoriteitpersoonsgegevens.nl/		
Has the Police been informed? (Cyber crime).		

Data Breach/Incident Reporting Register

Incident Reference	Date of Incident	Severity of Incident	Client	Reported to DDPA (AP)? Y/N	Open/ Closed.