NIKAL DATA PROTECTION POLICY

1. Purpose

1.1 This Policy defines requirements to ensure compliance with laws and regulations applicable to the Nikal' s collection, use, Processing, and transfer of Personal Data throughout the world.

2. Scope

2.1 Nikal is committed to complying with the applicable Data Privacy and Protection requirements in the countries in which it (the "Company") operates. Because of differences among these jurisdictions the Company has adopted a Data Protection policy, which creates a common core of values, policies and procedures intended to achieve generic compliance, supplemented (where applicable) with additional instructions and guidance applicable in those jurisdictions with unique requirements.

2.2 This policy is based upon the General Data Protection Regulation (GDPR), which operates within EU Regulation 2016/679, which provide a robust generic model for global Data Protection and privacy compliance.

2.3 This Policy applies to all Company full and part time employees and all suppliers and clients who receive Personal Data from the Company, have access to Personal Data collected or processed by the Company, or who provide information to the Company, regardless of geographic location.

2.4 As a policy commitment the Company will not process Personal Data without notification to the Data Protection authorities in jurisdictions, which require such notification. To ensure compliance with the regulations the Company will correctly establish its status for all Data Processing as either a Data Controller, or Data Processor acting for another Data Controller.

3. Company Compliance

3.1 The Company's data compliance program will be overseen by the Quality Controller of the company (QC).

3.2 The QC will implement the company's international Data Protection procedures of which:

3.2.1 Determining whether notification to one or more Data Protection authorities is required as a result of the Company's Data Processing activities, then making any required notifications, and keeping such notifications current.

3.2.2 Designing and implementing ongoing programs for training employees in Data Protection rules and procedures.

3.2.3 Establishing (with the involvement of the IT and legal departments) procedures and standard contractual provisions for obtaining compliance with this Policy by group companies, clients, suppliers, and third parties who receive Personal Data from the Company, have access to Personal Data collected or processed by the Company, or who provide information to the Company, regardless of geographic location.

3.2.4 Establishing mechanisms for periodic audits of compliance with this Policy, implementing procedures, and applicable law.

3.2.5 Establishing, maintaining, and operating a system for prompt and appropriate responses to Data Subject requests to exercise their rights.

3.2.6 Establishing, maintaining, and operating a system for the prompt and appropriate automatic disclosure to the relevant authorities and Data Subjects of any loss of Personal Data.

3.2.7 Informing the management of the Company of the potential corporate and Personal civil and criminal penalties which may be assessed against the Company and/or its employees for violation of applicable Data Protection laws.

3.2.8 Ensuring that the risk management plans in relation to Data Protection are implemented effectively and promptly.

3.2.9 Ensuring that adequate assurance regarding the effectiveness of Data Protection procedures and audits is provided to the Board, management and other stakeholders.

4. Data Protection Principles

4.1 The Company has adopted the following principles to govern its use, collection, and transmittal of Personal Data, except as specifically provided by this Policy or as required by applicable laws:

- Personal Data shall only be processed fairly and lawfully.
- Personal Data shall be obtained only for specified, explicit, lawful, and legitimate purposes, and shall not be further processed in any manner incompatible with those purposes.
- Personal Data shall be adequate, relevant and not excessive in relation to the purposes for which they are collected and/or processed.
- Personal Data shall not be collected or processed unless one or more of the following apply:
- The Data Subject has provided Consent.
- Processing is necessary for the performance of a contract directly with the Data Subject, or to which the Data Subject is an employee of a party;
- Processing is necessary for compliance with a Company legal obligation;
- Processing is necessary in order to protect the vital interests of the Data Subject;
- Processing is necessary for legitimate interests of the Company or by the third party or parties to whom the Data are disclosed, except where such interests are overridden by the fundamental rights and freedoms of the Data Subject.

Appropriate physical, technical, and procedural measures shall be taken to:

- Prevent and/or to identify unauthorised or unlawful collection, Processing, and transmittal of Personal Data; and
- Prevent accidental loss or destruction of, or damage to, Personal Data.

5. Transfers to Third Parties

5.1 Personal Data shall not be transferred to another entity, country or territory, unless reasonable and appropriate steps have been taken to establish and maintain the required level of Data Security.

5.2 Personal Data may be communicated to third persons only for reasons consistent with the purposes for which the Data were originally collected or other purposes authorised by law.

5.3 All transfers of Personal Data to third parties for further Processing shall be Subject to written agreements.

5.4 EU Personal Data shall not be transferred to a country or territory outside the European Economic Area (EEA) unless the transfer is made to a country or territory recognised by the EU as having an adequate level of Data Security or to the United States under the EU-US Privacy Shield to which the Company is registered.

5.5 Subject to the provisions of the above, Personal Data may be transferred where any of the following apply:

- The Data Subject has given Consent to the proposed transfer;
- The transfer is necessary for the performance of a contract between the Data Subject and the Company;
- The transfer is necessary for the conclusion or performance of a contract concluded in the interest of the Data Subject between the Company and a Third Party;
- The transfer is necessary or legally required on important public interest grounds, or for the establishment, exercise, or defence of legal claims;
- The transfer is required by law;
- The transfer is necessary in order to protect the vital interests of the Data Subject.

6. Prevention of Non-Complying IT Systems

6.1 The Company's Quality Controller shall establish a procedure for assessing the impact of any new or existing Technology on the privacy and security of Personal Data.

6.2 No new system or new version of an existing system shall be made available for use until the Quality Controller has obtained written confirmation from the IT Officer that there will no breach in the data protection.

7. Sources of Personal Data

7.1 Personal Data shall be collected only from the Data Subject unless the nature of the business purpose necessitates collection of the Data from other persons or bodies.

7.2 If Personal Data is collected from someone other than the Data Subject, the business unit collecting the Data must have confirmation, in writing, from the supplier of the Data that the Data Subject has provided Consent to the transfer to the Company.

8. Data Subject Rights

8.1 Data Subjects shall be entitled to obtain the information about their own Personal Data upon a request made in writing to the Quality Controller who will establish a system for logging each request under this Section as it is received and noting the response date

8.2 The Company shall provide its response to the above request within 40 days from the date of the written request, or within a shorter timescale if required by any country legislation.

8.3 Data Subjects shall have the right to require the Company to correct or supplement erroneous, misleading, out-dated, or incomplete Personal Data.

8.4 The Company may establish reasonable fees to cover the cost of responding to requests from non-employee Data Subjects.

9. Sensitive Data

9.1 Sensitive Personal Data should not be processed unless:

9.1.1 Such Processing is specifically authorised or required by law.

9.1.2 The Data Subject expressly and unambiguously Consents.

9.1.3 Where the Data Subject is physically or legally incapable of giving Consent, but the Processing is necessary to protect a vital interest of the Data Subject. This exemption may apply, for example, where emergency medical care is needed.

9.1.4 Data relating to criminal offenses may be processed only by or under the control of the Legal Department.

10. Data Quality Assurance

10.1 Personal Data must be kept only for the period necessary for permitted uses. The Company has established local Record Retention Policies, which determine applicable timescales for Data deletion.

10.2 Personal Data shall be erased if their storage violates any Data Protection rules or if knowledge of the Data is no longer required by the Company, or at the request of the Data Subject.

11. Third Party Processors

Where the Company relies on third parties to assist in its Processing activities, the Company will choose a Data Processor who provides sufficient security measures and take reasonable steps to ensure compliance with those measures, and in the case of any 3rd party within the US that they are also registered for the EU-US Privacy Shield.

12. Written Contracts for Third Party Processors

The Company shall enter into a written contract with each Data Processor requiring it to comply with Data privacy and security requirements imposed on the Company under local legislation.

13. Audits of Third Party Data Processors

As part of the Company's internal Data auditing process, the Company shall conduct periodic checks on processing by third party Data Processors, and in particular relating to the hand-off procedures for the Data especially in respect of security measures.

14. Notice to the Management of Potential Sanctions for Non-Compliance

14.1 The Quality Controller shall notify the management of the Company that:

14.1.1 Failure to comply with relevant Data Protection legislation may trigger criminal and civil liability, including fines, imprisonment, and damage awards; and

14.1.2 They can be personally liable where an offence is committed by the Company with their Consent or connivance, or is attributable to any neglect on their part.

15. Data Security

15.1 The Company has a Data Security Management policy, under which it shall adopt physical, technical, and organisational measures to ensure the security of Personal Data, including the prevention of their alteration, loss, damage, unauthorised Processing or access, having regard to the nature of the Data, and the risks to which they are exposed by virtue of human action or the physical or natural environment. These measures will be documented within the Data Security Policy, which will be reviewed at least annually, or when necessary to reflect significant changes to security arrangements.

15.2 Adequate security measures should include all of the following:

15.2.1 Prevention of unauthorised persons from gaining access to Data Processing systems in which Personal Data are processed.

15.2.2 Preventing persons entitled to use a Data Processing system from accessing Data beyond their needs and authorisations.

15.2.3 Ensuring that Personal Data in the course of electronic transmission during transport or during storage on a Data carrier cannot be read, copied, modified or removed without authorisation.

15.2.4 Ensuring that Personal Data are protected against undesired destruction or loss.

15.2.5 Ensuring that Data collected for different purposes can and will be processed separately.

15.2.6 Ensuring that Data are not kept longer than stipulated in the Data Retention Policy, including requiring that Data transferred to third persons be returned or destroyed.

16. Compliance Measurement

16.1 The Quality Controller shall establish a schedule for and implement a Data Protection compliance audit for all business units. The Quality Controller, in cooperation with the business units, shall create a plan and schedule for correcting any identified deficiencies within a fixed, reasonable time.

16.2 Each Company business unit shall review annually its Data collection, Processing, and Security practices and shall determine what Personal Data the business unit is collecting.

16.3 The information collected in this annual review shall be delivered to the Quality Controller for review and appropriate action including, without limitation, the following:

16.3.1 Making recommendations for improvement to policies and procedures in order to improve compliance with this Policy and applicable law.

16.3.2 Satisfying the requirements for self-certifying compliance within local Data Protection Authorities.

17. Implementation

17.1 This Policy shall be available to employees and an abridged public version shall be made available to others via the Company's website.

17.2 The Quality Controller, in cooperation with the Business Units, will develop a timeline and program for implementing this Policy.

17.3 This Policy may be revised at any time but at least annually by the QC. Notice of significant revisions shall be provided to employees and to all the relevant stakeholders. The Data Protection Policy shall always be available on the company's website.

18. Contacts

For any further information, please contact the Quality Controller at privacy@nikal.it .

Nicole Muratori
Managing Director
May 2018