Data Protection Policy

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 a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

Personal data processing: any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

Controller (or Data Controller): the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;

Processor (or Data Processor): a natural or legal person, public authority, agency or other body, which processes personal data on behalf of the controller;

Third party: a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data;

Personal data breach: 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;

Top Management Commitment

ELVAL, the Aluminium Rolling Division of ElvalHalcor S.A., is committed to protecting the personal data it processes as part of its business processes and operations, complying with international and local legislation, as well as good practices on personal data processing.

This policy applies to all personal data being processed by all ELVAL staff, external contractors, affiliates and other 3rd parties acting on behalf of ELVAL, the Aluminium Rolling Division of ElvalHalcor S.A., It applies to ELVAL activities either as Data Controller, Data Processor or both.

In line with 2016/679 General Data Protection Regulation of the EU ('GDPR'), ELVAL Top Management has introduced a data protection framework surrounding the processing of personal data, with the aim of adhering to the following principles:

- Personal data must be processed fairly, lawfully and transparently to the individuals whose data is being processed
- Personal data must be processed only where this is strictly necessary for legal, regulatory or other legitimate company purposes
- Processing of personal data must involve only the data required for these purposes and no further
- Processing must include accurate personal data
- Personal data must be processed only for the time needed to satisfy these purposes and no further
- The personal data being processed must be secured against unauthorised processing, loss of confidentiality, integrity or availability by implementing appropriate measures
- Individuals' defined rights on their personal data processing must be addressed

This present policy and supporting tools and documentation (collectively referred to as Data Protection Management System – DPMS), including, but not limited, the Records of Processing Activities, Data Protection Impact Assessments, Gap Analysis reports, associated data protection policies and procedures, as well as Privacy Enhancing Technologies (PETs) fulfil the accountability principle of EU GDPR. In this extent, processing of personal data must be governed by the DPMS.

Awareness

GDPR and other personal data related legal requirements must be integrated in the business activities of ELVAL.

ELVAL must ensure that the management of personal data as per the aforementioned principles becomes part of the business processes. Awareness on the principles of personal data management must be raised to staff that is involved in processing of personal data.

Responsibilities

The protection of personal data is the responsibility of all staff, contractors, affiliates and other 3rd parties acting on behalf of ELVAL. For the proper integration of personal data protection

requirements in the activities of ELVAL, appropriate assignment of personal data protection responsibilities is needed. ELVAL must designate a Data Protection Coordinator (DPC), working in cooperation with the Steelmet Data Protection Officer (DPO).

The responsibilities of the DPC include:

- Ensuring conformance to the policy
- Policy review
- Ensuring execution of risk assessment on processing activities
- Acting as a point of contact for data subjects and Supervisory Authorities
- Advising on the implementation of personal data protection measure
- Delivering awareness seminars on personal data protection
- Liaising with business and control functions on personal data protection issues
- Keeping up-to-date with changes to the legal, statutory and technological framework on personal data protection and applying appropriate changes
- Reviewing the implementation of the DPMS and recommending mitigation actions, where applicable
- Recommending DPMS updates to address changes in the applicable regulatory framework and to enhance the maturity level of the Group and companies surrounding the protection of personal data.
- Advising on the effective management of data breaches.

Recording & Risk-Assessing Processing Activities

ELVAL must maintain a Record of Processing Activities (RPA or record) that involves processing of personal data. Personal data processing outside the scope and activities recorded in the RPA is forbidden.

This record must at least contain for each activity:

- If the company operates as a Data Controller/ Processor or Joint Data Controller
- The purposes of the processing
- The legal basis for the processing
- The categories of personal data
- The categories of data subjects
- The categories of recipients of personal data
- Any transfers to other countries
- The retention requirements for each category of data

The Record of Processing Activities must be updated annually upon changes to the activities and the personal data used by the relevant business owner.

For activities where an initial estimation shows a possible high risk against data subjects due to these activities and the personal data being processed, a Data Protection Impact Assessment (DPIA) must take place. Such an assessment must also take place when designing of changing systems or having changes to existing non-high risk activities take place that denote a possible shift to high risk.

The assessment must at least contain:

- A description of the processing operation and its purposes
- An assessment of the need of processing personal data regarding the purposes
- An assessment of risks against data subjects
- The measures defined to address these risks

Owners must be identified for each risk and technical & organisational treatment options considered for implementation. Both risk assessment and treatment processes results must be documented.

Fair, Lawful and Transparent Processing

Personal data must be processed fairly, lawfully and transparently to the individuals whose data is being processed.

ELVAL must process personal data according to the requirement of lawfulness, as described by GDPR Article 6 and avoid processing special categories of personal data ('sensitive' personal data), except if the cases of GDPR Article 9 permit so.

At all times, individuals whose personal data is being processed must be clearly and concisely informed of such processing, the purposes related, the kinds of data, recipients, retention periods, any transfers outside the EEA, as well as their rights regarding the said processing, including the right to complain to a Supervisory Authority. Informing data subjects must take place prior to personal data processing.

Processing for Specific Legitimate Purposes

Personal data is to be processed only where this is strictly necessary for legal, regulatory or other legitimate company purposes.

The purposes must be specified and processing must not deviate from these purposes (purpose limitation), except if the new purpose adheres to the principles of legitimacy (e.g. legal obligation, communicated to the data subjects, consent etc.)

Consent, where needed, must be freely given, documented and retractable at any time.

Sharing of personal data for a legitimate purpose must include a clearly defined set of limitations on use and responsibilities on protecting the personal data. The use of shared personal data by the recipient must adhere to the defined purpose and the information originally given to the data subject.

Adequate Data Usage

Processing of personal data must involve only the data required for the defined purposes and no further, as prescribed by applicable legal or regulatory requirements or allowances.

The data collected must be sufficient for the intended purpose but not excessive. The usage of personal data for processing activities must ensure that the minimum of personal data is used for the intended purpose. In cases where the activity can be carried out with no personal data, then that data must be anonymised or deleted altogether in the case of an alternative method to carry out the purpose.

Accurate Data Usage

Processing must include accurate personal data.

Personal data integrity must be safeguarded. Personal data must be accurate and up-to-date. Data subjects must –where possible- have the ability to provide updated personal data.

Data Retention

Personal data must be processed only for the time needed to satisfy these purposes and no further.

Retention periods must be defined for personal data, based on specific criteria that must at all times include legal obligations to maintain data for a certain amount of time. At the end of the retention period, personal data must be disposed of with a level of security proportionate to the sensitivity of the personal data.

Security of Personal Data

The personal data being processed must be secure against unauthorised processing, loss of confidentiality, integrity or availability by implementing appropriate measures.

Technical and organisational security measures must be implemented for the security of personal data, according to a risk assessment of the processing activities, systems used, solution costs and technological ability. The aim of such measures must be to protect the confidentiality, integrity and availability of the personal data and the resiliency of the systems used to process it.

Measures must be implemented at the production, test and development systems, backup systems and media as well as non-electronic forms of personal data management (e.g. by implementing

physical security controls on paper media). Security must be applied both for the storage of personal data as well as for transmitting it for any use.

Organisational controls must include prompt security incident handling and reporting. The aim is threefold:

- Restore the data and systems to their proper operability
- Investigate root causes of the incident
- Examine impact and proceed with appropriate reporting, if so required

In the case where an incident may cause impact to a data subject, due to the personal data involved in the incident, the Supervisory Authority is to be notified within 72 hours. In the case where this risk is high, prompt plans must be made for informing the data subjects themselves. The Data Protection Coordinator of the company must be kept informed in all cases and during all phases of a security incident that constitutes personal data breach.

Checks must take place prior to divulging data to a 3rd party for any legitimate reason, in order to ascertain that the recipient will respect the individuals and protect their data. Especially in the case of contractors acting as Data Processors, assurances on the processing of the personal data must be committed through the relevant Data Processor Agreement. Also, it must be ensured that any requestors for such data are authenticated as authorised recipients first.

Data Subjects' Rights Management

Individuals' defined rights on their personal data processing must be addressed.

Data subjects are provided by the GDPR with certain rights that must be addressed by ELVAL. A data subject expressing in writing a request to exercise a right requires the company to first authenticate and then respond to any such request without undue delay and within one (1) month the latest. In cases where a request cannot be fulfilled within the set time limits, the data subject must be promptly informed, and the request addressed within another two (2) months.

The rights for data subjects are:

- Right to be Informed
- Right of Access
- Right to Rectification
- Right to Erasure
- Right to Restriction of Processing
- Right to Data Portability
- Right to Object
- Right against Automated Decision-Making, Profiling
- as well as the right to withdraw from a previously given consent to personal data processing

While there are cases where a request for the exercise of a data subject right may not be satisfied (e.g. in the case of overriding legal obligations of the company), all requests must be responded.

All rights, including the right to complain to a Supervisory Authority must be communicated beforehand to the data subject, prior to receiving (if possible) and processing its personal data – See 'Fair, Lawful and Transparent Processing' section.

Data Protection by Design and by Default

Personal data processing must be addressed in every processing activity from its inception and design through to its implementation and operation.

Protection of personal data must be part of any solution design, acquisition, development, change request and/or other operational activity. It must be part of the criteria used for the selection of vendors and third parties, management of projects, as well as risk management activities.

Policy Compliance Audit

To ensure that ELVAL and its staff comply with the provisions and requirements of this Policy, the DPC with the assistance of relevant roles (e.g. Information Security Officer) undertakes an annual (at least) compliance audit.

Upon completion of the audit, the DPC, in cooperation with the relevant departments and directorates, shall develop an action plan to correct and remedy any discrepancies found in the evaluation of the audit findings.

Subsequently, the DPC submits a DPMS report that at least includes the following:

- DPMS performance information (audit results, non-conformities, corrective actions etc.)
- Changes occurred in the DPMS since the last report
- Identified threats to the processing of personal data
- Information regarding the complaints and the data subjects' rights requests handling
- Any potential or recognized data breach incident