

**ELEKTROMETAL**  
**Spółka Akcyjna**  
43-400 Cieszyn, Stawowa 71

# **PERSONAL DATA PROTECTION POLICY IN ELEKTROMETAL SA**

valid from May 25 2018.

**The Personal Data Protection Policy was adopted under Regulation  
No.  
5/2018 of May 24, 2018.**

This document replaces the *"Personal Data Protection Policy and Manual of IT System Management in ELEKTROMETAL SA"* of May 27, 2015, adopted under the order of the Director General No. 01/2015.

Excerpt from *"Personal Data Protection Policy in Elektrometal SA"* – the document does not contain:

- Point 3 - PART B – INTERNALLY CLASSIFIED,
- Point 4 - PART C – CLASSIFIED,
- Point 6 - Appendices.

## Table of contents

|   |    |
|---|----|
| The Personal Data Protection Policy was adopted under Regulation No.....              | 1  |
| 1. Introduction .....   | 3  |
| 2. PART A – UNCLASSIFIED,.....  | 4  |
| 2.1 Scope of policy application .....   | 4  |
| 2.2 Definitions .....   | 5  |
| 2.3 Security of Personal Data Processing .....  | 8  |
| 2.4 The key principles of personal data protection implemented by the Controller..... | 9  |
| 2.4.1 Introduction .....  | 9  |
| 2.4.2 Lawfulness Principle .....  | 9  |
| 2.4.3 Principles of purposefulness and adequacy .....                                 | 10 |
| 2.4.4 Accuracy Principle .....  | 11 |
| 2.5 Exercise of the rights of individuals over the Controller.....                    | 11 |
| 2.5.1 Introduction .....  | 11 |
| 2.5.2 The right of access to Personal Data .....                                      | 13 |
| 2.5.3 The right to rectify Personal Data.....   | 14 |
| 2.5.4 The right to limit the processing of Personal Data .....                        | 14 |
| 2.5.5 The right to object .....   | 15 |
| 2.5.6 The right to transfer Personal Data.....  | 16 |
| 2.5.7 The right to be forgotten.....  | 16 |
| 2.6 Exercise of the obligation to provide information to natural persons,.....        | 17 |
| 2.6.1 Obligation to provide information .....   | 17 |
| 3. PART B – INTERNALY CLASSIFIED.....   | 20 |
| CONTENT NOT AVAILABLE .....   | 20 |
| 4. PART C – CLASSIFIED.....   | 20 |
| 5. Final provisions .....   | 20 |
| 6. Appendices .....   | 21 |
| CONTENT NOT AVAILABLE .....   | 21 |
| 7. Related documents.....   | 21 |

## 1. Introduction

1. The Personal Data Protection Policy is a document describing the Personal Data Protection policy applied by the Controller. It was developed in order for the Controller to implement the provisions of the Regulation of the European Parliament and of the Council (EU) 2016/679 of April 27, 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Official Journal of the EU L. 119 of May 4, 2016, p. 1).
2. The Protection Policy is divided into 3 parts according to the criterion of publicity of the content contained therein, i.e.: Part A – Unclassified, part B – internally classified, part C – classified.
3. Part A – unclassified, regulating the following issues:
  - a) Scope of application,
  - b) Definitions,
  - c) Security of processing of personal data,
  - d) The key principles of personal data protection carried out by the Controller,
  - e) Exercise of the rights of individuals over the Controller,
  - f) Exercise of the obligation to provide information to natural persons, accessible to all interested parties, including third parties over the Controller,
4. Part B – internally classified, regulating the following issues:
  - a) Processing of Personal Data in the Unit,
  - b) Responsibility for the implementation and adherence to the GDPR,
  - c) Authorisations for employees,
  - d) Incidents,
  - e) The responsibility of authorised persons,
  - f) Procedure for sharing Personal Data, only available to authorised persons,
5. Part C – classified, regulating the following issues:
  - a) Processing of Personal Data in the Unit,
  - b) Data Protection Coordinator,
  - c) Authorisation management and record of authorisations,
  - d) Risk Analysis,

- e) Register of Personal Data Processing activities,
- f) Register of Personal Data Protection incidents,
- g) Employee training,

only available to the Controller and persons designated by name by the Controller.

## 2. PART A – UNCLASSIFIED,

### 2.1 Scope of policy application

1. The Controller protects the rights and freedoms of natural persons by **implementing the right to protect Personal Data in connection with its processing.**
2. The protection applies to natural persons, regardless of their citizenship or place of residence, in connection with the Processing of Personal Data.
3. The Personal Data Protection Policy applies to the processing of Personal Data by the Controller in connection with the conducted activity.
4. The Policy together with the Appendices is a means of adapting the Controller to the requirements of the GDPR and applies to the Processing of Personal Data by the Controller:
  - a) in a fully or partially automated manner and
  - b) for non-automated (manual) Personal Data processing that constitutes part of a data set or is intended to form part of a data set.
5. The following are not covered by the scope of the GDPR and Policy:
  - a) data or sets of data that are not ordered according to specific criteria and their title pages,
  - b) processing of personal data by a natural person in the context of purely personal and home activities,
  - c) personal data of deceased persons,
  - d) processing of anonymous information (one that does not involve an identified or identifiable natural person) or personal anonymised data in such a way that data subjects cannot be identified at all or can no longer be identified; including processing for statistical or scientific purposes.

## 2.2 Definitions

The terms used in the policy shall be understood as:

1. **Personal Data Controller** or **Controller** or **PDA** – ELEKTROMETAL SA based in Cieszyn, Stawowa 71 (43-400 Cieszyn), which independently or jointly with others sets the purposes and methods of processing Personal Data,
2. **Anonymisation** – means the processing of Personal Data in such a way that it can no longer be attributed to the specific data subject by means of additional information or any other means available to the controller or processor. This operation is permanent and irreversible, which causes Personal Data not to be dealt with when it is conducted.
3. **Personal Data** – means all information regarding an identified or identifiable natural person (the data subject); an identifiable natural person is a person who can be directly or indirectly identified, in particular on the basis of an identifier such as name, identification number, location data, internet ID or one or more specific factors determining physical, physiological, genetic, psychological, economic, cultural or social identity of a natural person. At the same time, an identifiable person is an individual whose pseudonymised personal data can be assigned.
4. **Specific Personal Data** – means Personal Data including racial or ethnic origin, political views, religious or ideological beliefs, affiliation to trade unions and the processing of Genetic Data, Biometric Data to uniquely identify a person or Data relating to Health, sexuality or sexual orientation of that person, information on convictions and violations of law.
5. **Biometric data** – means personal data that results from special technical processing, relates to the physical, physiological or behavioral characteristics of a natural person and enables or confirms the unambiguous identification of that person, such as a facial image or fingerprint data.
6. **Health Data** – means personal data about the physical or mental health of a natural person - including the use of health care services - revealing information about his or her health.

7. **Department** – means an organisational unit separated by the Controller, along with all employees of this unit, which implements the tasks specified by the Controller and remaining in the relationship of subordination or supremacy to another organisational unit. The detailed division of the Unit into Departments contains the Organisational Chart currently applicable in the Unit.
8. **Incident** – means a breach of security of Personal Data leading to accidental or unlawful destruction, loss, modification, unauthorised disclosure or unauthorised access to Personal Data sent, stored or otherwise processed.
9. **IT Specialist** – means an Employee whose scope of duties includes at least supervision of an IT system in force at the Controller's or bearing responsibility for its proper operation. In the case of several employees meeting the above criterion, the term IT specialist applies to each of these employees.
10. **Unit** – means an organised enterprise run by the Controller.
11. **Recipient of Data** or **Recipient** – means a natural or legal person, public body, unit or other entity to which the Personal Data is disclosed, regardless of whether it is a Third Party. Public bodies that may receive Personal Data as part of a specific proceeding under Union law or the law of a Member State shall not, however, be considered as recipients; the processing of this data by these public authorities must be in accordance with the data protection rules applicable to the purposes of the processing.
12. **Restriction of Processing** – means a temporary ban on the further processing of Personal Data, excluding storage operations of such Personal Data and other operations carried out with the expressed consent of the data subject.
13. **Supervisory Authority** – means an independent public body established by Act 2018 or established by another EU Member State.
14. **Authorised Person** – a natural person acting under the authority of the Controller who has access to Personal Data and processes it only at the Controller's request with respect to the authorisation granted.
15. **Personnel or Employee** – a natural person remaining in an employment relationship with the Controller or in other permanent civil legal relationship. For the purposes of the Policy, interns, trainees, volunteers, and students on apprenticeship are also considered to be employees.

16. **Processing Entity** – means any entity that processes Personal Data on behalf of the Controller.
17. **Policy** – this is understood as the Personal Data Protection Policy with all Appendices.
18. **Personal Data Processing or Processing** – any operation or set of operations performed on Personal Data or personal data sets in an automated or non-automated way, such as: collecting, saving, preserving, organising, storing, adapting or modifying, downloading, viewing, using, disclosing by sending, distributing or otherwise sharing, matching or combining, limiting, deleting or destroying,
19. **Pseudonymisation** – means the processing of Personal Data in such a way that it can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is covered by technical and organisational measures that prevent them from being assigned to an identified or identifiable natural person. This operation is reversible, as opposed to Anonymisation.
20. **GDPR** – Regulation (EU) 2016/679 of the European Parliament and Council of April 27, 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Official Journal of the EU L. 119 of May 4, 2016, p. 1).
21. **Third Party** – means any natural or legal person, public authority, unit or entity other than the data subject, Controller, processor or persons who, under the authority of the controller or processor, may process personal data.
22. **IT System or Enterprise System** – means a set of cooperating devices, programs, information processing procedures and software tools used for Data Processing.
23. **Information society service** – means a service within the meaning of art. 1 point 1 letter b) of Directive of the European Parliament and of the Council (EU) 2015/1535.
24. **User** – means an Authorised Person who has the right to work in the IT System within the scope of the authorisation granted.

25. **Personal Data Collection** – means an ordered set of Personal Data available according to specific criteria, regardless of whether the set is centralised, decentralised or distributed functionally or geographically.
26. **Consent** – means voluntary, specific, conscious and unambiguous representation of the will, to which the data subject, in the form of a declaration or a clear confirmation action, authorises the processing of his/her Personal Data. The consent may be granted by a person after exceeding the minimum age indicated in the GDPR and Act of 2018. Silence, checkboxes selected by default, and actions not taken do not mean consent.

### 2.3 Security of Personal Data Processing

1. Through the security of Personal Data Processing, the Controller understands assuring:
  - a) confidentiality – a characteristic that ensures that Personal Data is not shared with unauthorised parties,
  - b) integrity – a characteristic that ensures that Personal Data is not altered or destroyed in an unauthorised manner,
  - c) availability – a characteristic that ensures that the Controller has not lost control over Personal Data, nor has he/she lost access to stored Personal Data,
  - d) accountability – a characteristic that ensures that the activities of the Controller and/or the Authorised Person and/or the User can be assigned only explicitly to the Controller and/or the Authorised Person and/or the User.
2. The Controller implements the necessary security measures: technical (including physical), organisational (including personal) and IT security measures to process Personal Data in accordance with the GDPR. The Controller submits the measures used to periodic reviews and updates.
3. When implementing the necessary security measures, the Controller ensures that the following rules are met:
  - a) purpose limitation – through collection for specific, explicit and legitimate purposes, and not in a manner inconsistent with these purposes;
  - b) Personal Data Minimisation – through processing the data adequately, appropriately and only to the extent that it is necessary for the purposes for which it is processed.



4. The Controller and his/her employees take into account the protection of Personal Data at every stage of the implementation of their activities, including also at the design stage of their services, products and business solutions.
5. The Controller is not obliged to appoint a personal data protection inspector in accordance with art. 37 of the GDPR.
6. In order to ensure effective implementation of the duties of the Controller on the protection of personal data and to ensure that individuals can exercise their rights, the Controller ensures proper entrustment of personal data protection tasks in the organisational structure of the Unit and ensures efficient and rapid flow of information on Personal Data protection. To this end, the Controller appoints the Personal Data Coordinator in accordance with the principles set out in § 4.2 of the Policy.
7. When undertaking actions and decisions concerning the protection of Personal Data Processing, the Controller consults the appointed Personal Data Coordinator.

## **2.4 The key principles of personal data protection implemented by the Controller**

### **2.4.1 Introduction**

1. The Controller and his/her employees Processing Personal Data ensure that the following rules for the protection of Personal Data are observed.
2. The processing of Personal Data takes place within the scope of economic activity performed by the Controller and within the scope of objectives implemented by the Controller within the existing organisational structure, including the activities of Departments designated for that purpose.
3. The application of the Protection Policy is complementary to the Controller's procedures in force defined by the ISO standards.

### **2.4.2 Lawfulness Principle**

1. Personal data in the Unit can only be processed on the basis of:
  - a) the statement of the data subject (consent),
  - b) the provision of law if it is necessary to fulfill the legal obligation of the Controller,

- c) the contract, if it is necessary for the performance of the contract, and the data subject is a party to the contract or if it is necessary to take action before the conclusion of the contract at the request of the data subject,
  - d) the legally justified interest of the Controller or the Third Party, if it is necessary for the attainment of that interest, and therefore the interest is not overridden by the fundamental rights or freedoms of the data subject.
2. In the business activity run by the Controller, the following fundamentals of the Personal Data Processing are distinguished, of which the Controller is the Controller:
    - a) provision of the law – in relation to the employees' personal data,
    - b) contract – in relation to Personal Data of contractors who run a sole proprietorship,
    - c) legitimate interest – in relation to Personal Data concerning the register of incoming and outgoing correspondence.
  3. Controller indicates the key features of Personal Data Processing in the Record of Processing Activities.

#### **2.4.3 Principles of purposefulness and adequacy**

1. Personal Data Processing can only take place for clearly identified and specific purposes.
2. Processed Personal Data must be adequate to the purpose for which it is collected, which means that it is possible to process only the data that is necessary for a particular purpose. In other words, without Processing this data, it is not possible to accomplish the goal.
3. The Controller indicates the key features of Personal Data Processing in the Record of Processing Activities.
4. The Controller together with his/her Employees [*once every two years or on the Controller's order*] conducts a review of the Processed Personal Data in terms of the purposefulness of its further Processing.
5. In the event of a change and/or establishment of a new Processing Objective, a test should be carried out whether a reagreement or a change of the Contract on Personal Data Processing is required.
6. The processing of Personal Data for purposes other than those for which it was collected is acceptable only if these purposes are compatible with each other.

#### **2.4.4 Accuracy Principle**

1. Personal Data Processed must be factually correct, which means that the data must reflect the actual state.
2. If the Controller has any doubts as to the validity of the Personal Data being processed, the Controller shall take all reasonable steps to verify the Personal Data.
3. All reasonable measures should be understood as the means available to the Controller to verify that the processed personal data remains true (current). The Controller is not obliged to take actions that require excessive costs or time or undertaking of actions which are not likely to update the Personal Data processed.
4. Until the Personal Data as to which the Controller has been doubtful is verified, the Controller should refrain from its further use.
5. In the event that the actions taken did not result in the updating of Personal Data, the Controller may delete false Personal Data.

### **2.5 Exercise of the rights of individuals over the Controller**

#### **2.5.1 Introduction**

1. The Controller provides the data subject with information about the processing of his/her Personal Data, in the manner and in the content indicated in this paragraph and covered by Appendix 1 "Information on the processing of personal data".
2. The Controller enables the data subject to exercise the right to:
  - a) access to his/her processed Personal Data (Art. 15 of the GDPR),
  - b) application for rectification or supplementation relating to the Personal Data (Art. 16 of the GDPR)
  - c) deletion of Personal Data (Art. 17 of the GDPR),
  - d) restriction on the processing of personal data (Art. 18 of the GDPR),
  - e) notification, at any time, of opposing to the processing of personal data (Art. 21 of the GDPR),
  - f) transfer of Personal Data (Art. 20 of the GDPR).

3. The Controller does not apply the method of automated decision-making in individual cases (Art. 22 of the GDPR), including profiling, therefore, natural persons are not entitled to not be subject to such decisions.
4. The Controller facilitates the data subject to exercise of his/her rights, except when the Controller shows that he/she is unable to identify the data subject who reports his/her rights. In such case, the Controller will, if possible, inform the person with the request to provide additional information to identify him/her.
5. The data subject directs to the Controller a request in matters regarding his/her rights, indicated in point 2 above in the form of:
  - a) writing – to the following address: President of the Management Board, 43-400 Cieszyn, Stawowa 71, or
  - b) electronically – to: rodo@elektrometal.com.pl, if the personal data is processed electronically.
6. The Controller provides the natural person whose data relate to information about actions taken by the Controller at the request of that person in matters regarding his/her rights in the period of:
  - a) without undue delay, but no later than one (1) month after receiving the request, or
  - b) extended by another two (2) months, due to the complex nature of requests or number of requests, about which the Controller informs the natural person within one (1) month giving the reason for the delay.
7. The Controller provides the natural person with information that he/she does not take action, at the request of that person in matters relating to his/her rights, one (1) month after receiving the request at the latest, together with:
  - a) stating the reasons for not taking action, and
  - b) instruction on the possibility of submitting a complaint to the Supervisory Body, and using legal protection measures before a court.
8. The use by natural persons of the rights referred to in paragraph 2 above is free of charge.
9. The Controller is obliged to notify about rectification, removal or limitation of Processing, to each Recipient to whom he/she disclosed Personal Data, unless this proves impossible or will require a disproportionately large effort. The template of the notification referred to in the preceding sentence is Appendix 13 "Template

of the Recipient's notification". The Controller informs the data subject about these Recipients if the data subject requests it.

### **2.5.2 The right of access to Personal Data**

1. At the request of the data subject, the Controller confirms that the Personal Data of that natural person is being processed.
2. The Controller provides the natural person with access to their Personal Data and the opportunity to obtain information on:
  - a) the processing purposes,
  - b) the categories relevant to Personal Data,
  - c) the recipients or categories of recipients to whom personal data have been or will be disclosed,
  - d) if possible, the planned period of storage of Personal Data, and if this is not possible, criteria for determining this period,
  - e) the rights of natural persons, as indicated in paragraph 2.5.1 point 2 of the Policy;
  - f) the right to submit a complaint to the Supervisory Body,
  - g) if the Personal Data was not collected from the data subject - all available information about their source.
3. The Controller provides the data subject free of charge with one copy of Personal Data subject to processing. For any subsequent copies requested by a natural person, the Controller may charge a flat fee of PLN 15, resulting from administrative costs including the cost of preparation, printing and delivery of the copy to the natural person. The right to obtain a copy of your Personal Data may not adversely affect the rights and freedoms of other natural persons.
4. If the data subject asks for a copy electronically, and unless otherwise indicated, the information is provided by electronic means.
5. The access right can be exercised by:
  - a) sending an e-mail to the following e-mail address: [rodo@elektrometal.com.pl](mailto:rodo@elektrometal.com.pl),
  - b) sending written notification to the following address: President of the Board, 43-400 Cieszyn, Stawowa 71,
  - c) filling a dedicated form located on the website: <http://www.elektrometal.eu>.

### **2.5.3 The right to rectify Personal Data**

1. At the request of the data subject on the rectification of Personal Data, addressed to the Controller, the Controller immediately corrects the Personal Data that relate to the data subject and are incorrect.
2. Taking into account the purposes of processing, the data subject has the right to request supplementing incomplete personal data, including by submitting an additional statement.
3. The right to rectification can be exercised by:
  - a) sending an e-mail to the following e-mail address: [rodo@elektrometal.com.pl](mailto:rodo@elektrometal.com.pl),
  - b) sending written notification to the following address: President of the Board, 43-400 Cieszyn, Stawowa 71,
  - c) filling a dedicated form located on the website: <http://www.elektrometal.eu>.

### **2.5.4 The right to limit the processing of Personal Data**

1. At the request of the data subject about restricting the processing of Personal Data, the Controller limits the processing in the following cases:
  - a) the data subject questions the correctness of Personal Data - for a period allowing the Controller to check the correctness of such data;
  - b) The processing is unlawful and the data subject opposes the removal of Personal Data, requesting instead to limit its use;
  - c) The Controller no longer needs Personal Data for processing purposes, but they are needed by the data subject to determine, assert or defend claims;
  - d) the data subject has submitted an objection (pursuant to Article 21 sec. 1 of the GDPR) referred to in § 2.5.5 - until it is determined whether the legitimate grounds on the part of the Controller are overriding the grounds for objection of the data subject concern.
2. The consequence of the Processing limiting is that the Personal Data covered by the limit may only be stored by the Controller. All other operations of the Controller may be performed only:
  - a) with the consent of the data subject, or
  - b) in order to determine, assert or defend claims, or
  - c) in order to protect the rights of another natural or legal person.

3. The Controller informs the person who requested the restriction on revoking the restriction before further processing of his/her Personal Data.
4. The right to limit the processing of personal data can be exercised by:
  - a) sending an e-mail to the following e-mail address: [rodo@elektrometal.com.pl](mailto:rodo@elektrometal.com.pl),
  - b) sending written notification to the following address: President of the Board, 43-400 Cieszyn, Stawowa 71,
  - c) filling a dedicated form located on the website: <http://www.elektrometal.eu>.

### **2.5.5 The right to object**

1. In the event that the processing of Personal Data is necessary for the purposes resulting from the legally legitimate interests pursued by the Controller or by a Third Party, a natural person may object to such Processing, citing the reasons related to his/her specific situation.
2. Submitting an objection with a justification by a natural person results in the prohibition of further processing of Personal Data, unless the Controller demonstrates that his/her legitimate interests override the interests, rights and freedoms of the data subject or further processing of Personal Data will be carried out solely for the purpose of determination, investigation or defense of claims.
3. At the request of the data subject, including opposition to the processing of Personal Data for direct marketing purposes, the Controller is no longer allowed to process Personal Data for direct marketing purposes, to the extent that the processing is related to such direct marketing.
4. The Controller is obliged, at the latest on the occasion of the first communication with the data subject, to clearly inform separately from any other information about the right to object, referred to in point 3 above (direct marketing).
5. The right to object can be exercised by:
  - a) sending an e-mail to the following e-mail address: [rodo@elektrometal.com.pl](mailto:rodo@elektrometal.com.pl),
  - b) sending written notification to the following address: President of the Board, 43-400 Cieszyn, Stawowa 71,
  - c) filling a dedicated form located on the website: <http://www.elektrometal.eu>.

### 2.5.6 The right to transfer Personal Data

1. The data subject has the right to receive, in a structured, commonly used, machine-readable format, Personal Data concerning him/her that he/she provided to the Controller, and has the right to send this Personal Data to another Controller without any hindrance from the Controller, if both of the following conditions are met:
  - a) the processing is carried out on the basis of **Consent** to Personal Data Processing or Processing takes place on the basis of the **Contract** and
  - b) the processing is carried out in an **automated manner**.
2. At the request of the data subject about the sending of Personal Data by the Controller directly to another Controller, the Controller sends this Personal Data to the indicated Controller, if it is technically possible.
3. The exercise of the right referred to in section 1 of this article, is without prejudice to the right to delete Personal Data.
4. The right to transfer Personal Data may not adversely affect the rights and freedoms of others.
5. The right to transfer Personal Data can be exercised by:
  - a) sending an e-mail to the following e-mail address: [rodo@elektrometal.com.pl](mailto:rodo@elektrometal.com.pl),
  - b) sending written notification to the following address: President of the Board, 43-400 Cieszyn, Stawowa 71,
  - c) filling a dedicated form located on the website: <http://www.elektrometal.eu>.

### 2.5.7 The right to be forgotten

1. The data subject has the right to demand from the Controller the immediate removal of all processed Personal Data if:
  - a) they are no longer needed for specific purposes,
  - b) the person has withdrawn his/her consent and there is no other reason,
  - c) the person has submitted an objection and there is no exception referred to in § 2.5.5 point 2 of the Policy,
  - d) personal data is processed unlawfully,
  - e) the obligation to remove is provided for by law,
  - f) data has been collected in connection with Information Society Services.



2. Despite the request to delete all processed Personal Data immediately, the Controller may further Process Personal Data if it is:
  - a) necessary for the Controller to meet his/her legal obligation to require processing under the law,
  - b) necessary to establish, assert or defend claims.
3. The right to be forgotten can be exercised by:
  - a) sending an e-mail to the following e-mail address: [rodo@elektrometal.com.pl](mailto:rodo@elektrometal.com.pl),
  - b) sending written notification to the following address: President of the Board, 43-400 Cieszyn, Stawowa 71,
  - c) filling a dedicated form located on the website: <http://www.elektrometal.eu>.

## **2.6 Exercise of the obligation to provide information to natural persons,**

### **2.6.1 Obligation to provide information**

1. When collecting Personal Data directly from the person whom the data relates to, the Controller provides him/her with all the following information, indicating the letter with the term "INFORMATION ON PROCESSING OF PERSONAL DATA":
  - a) his/her identity (company/name, registered office, KRS number) and contact details (mailing address, telephone number, e-mail address);
  - b) purposes of Personal Data Processing, and the legal basis of the Processing;
  - c) if the processing is carried out on the basis specified in § 2.4.2, point 2 c) of the Policy - legitimate interests pursued by the Controller,
  - d) the information about the recipients of personal data or categories of recipients, if any,
  - e) the period during which Personal Data will be stored, and if this is not possible, the criteria for determining that period;
  - f) information about the right to request from the Controller access to Personal Data relating to the data subject, its rectification, removal or limitation of Processing or the right to object to the Processing, as well as the right to transfer Personal Data;
  - g) if the Processing is based on Consent - information about the right to withdraw the Consent at any time without affecting the legality of the Processing which was made on the basis of the Consent prior to its withdrawal;
  - h) information about the right to submit a complaint with the Supervisory Body;

- i) information whether the provision of Personal Data is a statutory, contractual or pre-contractual requirement and whether the data subject is obliged to provide it and what are the consequences of not providing the data.
2. The obligation to provide information is exercised:
    - a) in writing or otherwise, including, where appropriate, electronically; which applies in particular when personal data is processed electronically, possibly
    - b) verbally, but only if: the data subject requests verbal information, and in other ways the Controller will confirm the identity of the data subject.
  3. If the Personal Data was not obtained from the data subject, the Controller provides the following information to this person:
    - a) his/her identity and contact details,
    - b) where applicable - IODO (Personal Data Protection Inspector) contact details,
    - c) the purposes of the Processing for which the Personal Data is to be used, and the legal basis for its Processing,
    - d) categories of relevant Personal Data (*name, surname, PESEL number, invoice number, etc.*),
    - e) information on the Recipients or on the categories of Recipients, if any,
    - f) the period during which Personal Data will be stored, and if this is not possible, the criteria for determining that period;
    - g) if the processing is carried out on the basis specified in § 2.4.2 point 2 c) of the Policy - provides and explains legally justified interests pursued by the Controller or by a Third Party,
    - h) information about the right to request from the Controller access to Personal Data relating to the data subject, its rectification, removal or limitation of Processing or the right to object to the Processing, as well as the right to transfer Personal Data;
    - i) if the Processing is based on Consent - information about the right to withdraw the Consent at any time without affecting the legality of the Processing which was made on the basis of the Consent prior to its withdrawal;
    - j) information about the right to submit a complaint with the Supervisory Body,
    - k) the source of Personal Data, and if applicable - whether it comes from publicly available sources.
  4. The Controller shall provide the information referred to in point 3 above:

- a) within a reasonable time after receiving Personal Data - at the latest within one month of being disclosed by another entity,
  - b) if Personal Data is to be used to communicate with the data subject  
- at the latest at the first such communication with that person, or
  - c) if it is planned to disclose Personal Data to another Recipient - at the latest at its first disclosure.
5. In the event of a change in the information that has been provided to the data subject, the Controller shall promptly renew the obligation to provide information by providing new or changed information. In such case, the rules on providing information to natural persons referred to in sections 1 – 4 above apply accordingly. The update of the Personal Data Processing Information may be sent by e-mail, provided that the natural person has provided such an address for correspondence.

### **3. PART B – INTERNALY CLASSIFIED**

**CONTENT NOT AVAILABLE**

### **4. PART C – CLASSIFIED**

**CONTENT NOT AVAILABLE**

### **5. Final provisions**

1. Any Person Authorised to Process Personal Data is required to read part [A] and [B] of Protection Policy and make a relevant statement confirming knowledge of its content before being allowed to process Data.
2. Notwithstanding the provisions of section 1 above, persons exercising control over strategic processes at the Controller's are required to read part [C] of the Protection Policy and make a relevant statement confirming the knowledge of its content before being allowed to process Data.
3. Subject to Part [A], the Protection Policy is an internal document and may not be made available to unauthorised persons or institutions in any form without prior written consent of the Controller. Part [A] of the Protection Policy is published on the <http://www.elektrometal.eu> website.
4. The Protection Policy Document may be presented to outsiders and institutions without the consent of the Controller, if at the same time the content of information on the applicable Personal Data safeguards is not disclosed (after showing the appropriate documentation).
5. In matters not covered by the Protection Policy, the provisions of the GDPR apply.
6. The Protection Policy enters into force on the day it is signed by persons representing the Controller.
7. Any changes to the Protection Policy are made in the form of an updated Protection Policy document, with the date of the update.

## 6. Appendices

**CONTENT NOT AVAILABLE**

## 7. Related documents

1. *"Personal traffic instructions in force at ELEKTROMETAL SA in Cieszyn"*
2. Instruction QI050102 – *"Instructions for securing data on electronic media"*
3. Instruction QI050103 – *"Office and archival instructions"*

The Management Board of Elektrometal SA

Chairman of the Board – Andrzej Wojtyła

/-----/  
.....

Board Member – Bogusław Kapcia

/-----/  
.....

Cieszyn, May 24, 2018