EEA Personal Data Protection Rules

Part I General Provisions

Article 1 (Purposes and Applications)

1.1 These rules (these "**Rules**") are intended to ensure compliance with the General Data Protection Regulation ("**GDPR**") in circumstances where the GDPR applies to us, and to ensure compliance with the regulations on the cross-border transfer of Personal Data (as defined below in Article 2, item (2)) to which the GDPR applies.

1.2 These Rules do not change the content of our internal rules based on the laws other than GDPR.

1.3 If there is any conflict between these Rules and our internal rules based on the laws other than GDPR, the provision that imposes a heavier obligation to protect Personal Data shall prevail.

1.4 Among these Rules, Part II applies only to the Processing of Personal Data to which the GDPR applies.

Article 2 (Definitions)

The definition of the terms used in these Rules shall be as follows:

(1) "**EEA member states**" means states within the European Economic Area.

(2) "**Personal Data**" means any information relating to an identified natural person or identifiable natural person (the "**Data Subject**") who can be identified directly or indirectly by reference to an identifier such as a name, an identification number, location data, an online identifier (including IP address, Cookie), or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

(3) "**Sensitive Data**" means Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership and genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health, or data concerning a natural person's sex life or sexual orientation.

(4) "**Processing**" means any operation or set of operations that 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.

PART II Processing of Personal Data to which the GDPR Applies

Chapter I Processing of Personal Data

Article 3 (General Principles Relating to the Processing of Personal Data)

3.1 Personal Data shall be processed pursuant to the following principles:

(1) processed lawfully, fairly and in a transparent manner in relation to the Data Subject;

(2) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;

(3) adequate, relevant and limited to the extent necessary in relation to the purposes for which they are processed;

(4) accurate and, where necessary, kept up to date;

(5) kept in a form that enables identification of the Data Subjects for no longer than is necessary for the purposes for which the Personal Data is processed; and

(6) processed in a manner that ensures appropriate security of the Personal Data using appropriate technical or organizational measures.

3.2 We will maintain Personal Data Processing in compliance with the preceding paragraph 3.1 in a condition available for demonstration.

Article 4 (Processing of Personal Data)

Personal Data shall not be processed except if one of the following applies:

(1) the Data Subject has given consent to the Processing of his or her Personal Data for specific purpose(s);

(2) Processing is necessary for the performance of a contract to which the Data Subject is party or in order to take steps at the request of the Data Subject prior to entering into a contract;

(3) Processing is necessary for compliance with a legal obligation set forth under the laws and regulations of the EU or the EEA member states to which we are subject;

(4) Processing is necessary in order to protect the vital interests of the Data Subject or another natural person;

(5) Processing is necessary for the purposes of the legitimate interests pursued by us or by a third party (except where such interests are overridden by the interests or fundamental rights and freedoms of the Data Subject which require protection of Personal Data); or

(6) other cases where the Processing is permitted under the laws and regulations of the EEA member states, especially for employment-related purposes where necessary for hiring decisions or, after hiring, for carrying out or terminating the employment contract.

(7) where the personal data are further processed for purposes other than those for which they were collected (however, prior to such further processing, the Data subject must be informed about the purpose).

Article 5 (Conditions for Consent)

If the Processing of Personal Data is legally based on consent, the consent must be freely given by the Data Subject through a clear and affirmative act after being clearly and specifically informed about the processing. Withdrawing consent must be as easy as giving consent. we shall be able to demonstrate that the Data Subject has withdrawn her/his consent.

Article 6 (Processing of Sensitive Data)

6.1 Irrespective of the provisions of Article 4, Sensitive Data shall not be processed except in the following cases:

(1) the Data Subject has given explicit consent to the Processing of Sensitive Data for specified purposes;

(2) the Processing is necessary for the purposes of carrying out the obligations and exercising specific rights of ours or the Data Subject in the field of employment and social security and social protection law in so far as such Processing is approved by the laws and regulations of the EU or the EEA member states, or collective agreements in accordance with the laws and regulations of the EEA member states that stipulate appropriate safeguards relating to the fundamental rights and interests of the Data Subject;

(3) the Processing is necessary to protect the vital interests of the Data Subject or of another natural person where the Data Subject is physically or legally incapable of giving consent;

(4) the Processing relates to Personal Data which are manifestly made public by the Data Subject;

(5) the Processing is necessary for the establishment, exercise or defense of legal claims;

(6) the Processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health care or social care or treatment or the management of health care systems or social care systems and social care services on the basis of the laws and regulations of the EU or the EEA member states or pursuant to contract with a health professional and subject to the conditions and safeguards set forth in the GDPR; or

(7) other cases where the Processing is authorised under the laws and regulations of the EEA member states.

6.2 "Conditions provided in the GDPR" provided in preceding Article 6.1, item (6) shall mean that Sensitive Data are processed by or under the responsibility of a professional subject to the obligation of professional secrecy under EU law or the laws of the the EEA member states or rules established by national competent bodies or by another person also subject to an obligation of secrecy under the laws and regulations of the EU or the EEA member states or rules established by national competent bodies.

Article 7 (Collecting Personal Data from the Data Subject)

7.1 Where Personal Data are collected from the Data Subject, in principle, we will provide the Data Subject with the information in each item below upon such collection.

(1) The name and the contact details of ours and the EU representative (if it has been appointed) and the contact details of the data protection officer (if it has been appointed);

(2) the purposes of and the legal basis for the Processing of Personal Data;

(3) where the Processing of Personal Data is based on Article 4, item (6), the legitimate interests pursued by us or by a third party;

(4) where the Personal Data is provided to any third party, the recipients or categories of recipients of the Personal Data;

(5) where we intend to transfer the Personal Data to any third party located in a third country outside the EEA, such fact, and the existence or absence of an adequacy decision on the transferee by the Commission, or in the case of transfers under Article 11, paragraph 1, item (2) or Article 11, paragraph 4, item (7), appropriate or suitable safeguards and the means by which to obtain a copy of the documents indicating the details of such safeguards (standard contractual clauses in the case of transfers under Article 11, paragraph 1, item (2));

(6) the period for which the Personal Data will be stored (if that is not possible, the criteria used to determine that period);

(7) the existence of the right to request access to and rectification or erasure of Personal Data or restriction of Processing or to object to Processing as well as the right to data portability;

(8) where the Processing of Personal Data is based on Article 4, item (1) or Article 6, paragraph 1, item (1) (Data Subject's Consent), the existence of the right to withdraw consent at any time, without affecting the lawful Processing based on consent before its withdrawal;

(9) the right to lodge a complaint with a supervisory authority;

(10) whether the provision of Personal Data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the Data Subject is obliged to provide the Personal Data and of the possible consequences of failure to provide such data; and

(11) the existence of automated decision-making, including profiling, and at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such Processing for the Data Subject.

7.2 Where we carry out further Processing for purposes other than the purposes for which the collected Personal Data was collected, we will provide to the Data Subject the information relating to such other purposes, and the information set forth in items (6) through (11) of the preceding paragraph before such further Processing is carried out.

7.3 The preceding paragraphs shall not apply if the Data Subject already holds the information set forth in the preceding paragraphs.

Article 8 (Collecting Personal Data from Persons Other than the Data Subject)

8.1 Where we collect Personal Data from persons other than the Data Subject, we will in principle provide the Data Subject with the information in each item below upon such collection:

(1) the information provided in preceding Article, paragraph 1, items (1) through (9), and (11);

(2) the categories of Personal Data to be collected; and

(3) the source of Personal Data and the fact that the source is publicly accessible, if applicable.

8.2 The period in which we provide the Data Subject with the information set forth in the preceding paragraph shall be within a reasonable period after obtaining the Personal Data, within one month in principle. However, if any of the items below applies, then up to the time set forth in each item below.

(1) If the Personal Data are to be used for communication with the Data Subject, at the latest at the time of the first communication to that Data Subject; or

(2) if the disclosure of Personal Data to a third party is envisaged, at the latest when the Personal Data are first disclosed.

8.3 Where we further process the Personal Data for a purpose other than that for which the Personal Data were obtained, we will provide the Data Subject prior to that further Processing with information on that other purpose and with any relevant further information set forth in paragraph 1, item (3), and preceding Article, paragraph 1, items (6) through (9) and (11).

8.4 The preceding paragraphs shall not apply where and insofar as:

(1) the Data Subject already has the information;

(2) the provision of such information proves impossible or would involve a disproportionate effort;

(3) the obligations for obtaining the information or disclosure are expressly laid down by EU law or domestic laws of the EEA member states to which we are subject and which provides appropriate measures to protect the Data Subject's legitimate interests; or

(4) where the Personal Data must remain confidential subject to an obligation of professional secrecy regulated by EU law or domestic laws of the EEA member states, including a statutory obligation of secrecy.

Article 9 (Joint Controllers)

9.1 Controllers who jointly determine the purposes and means of processing with us shall be joint controllers. We and the controllers who jointly determine the purposes and means of processing with us shall in a transparent manner determine their respective responsibilities for compliance with the obligations under these Rules, in particular as regards the exercise of rights of the Data Subject referred to in chapter II and their respective duties to provide the information referred to in paragraph 9, item (1) and paragraph 8, item (1), by means of an arrangement between the controllers unless, and in so far as, the respective responsibilities of us and the controllers who jointly determine the purposes and means of processing with us are determined by Union or Member State law to which the controllers are subject. The arrangement may designate a contact point for data subjects.

9.2 The arrangement referred to in paragraph 1 shall duly reflect the respective roles and relationships of us and the controllers who jointly determine the purposes and means of processing with us vis-à-vis the data subjects. The essence of the arrangement shall be made available to the data subject.

9.3 Irrespective of the terms of the arrangement referred to in paragraph 1, the data subject may exercise his or her rights under these Rules in respect of and against us and the controllers who jointly determine the purposes and means of processing with us.

Article 10 (Outsourcing of Personal Data Processing)

10.1 In the case of entrusting Personal Data Processing to any third party (the counterparties to whom such Processing is entrusted shall be the "**Entrusted Parties**"), we shall only use the Entrusted Parties that meet the requirements of the GDPR and provide sufficient guarantees for the implementation of technical and organisational measures, and shall ensure the rights of the Data Subject are protected by the Entrusted Parties.

10.2 In the case of entrusting Personal Data Processing to any external third party, the contract that sets out the subject-matter and duration of the Processing, the nature and purpose of the Processing, the type of Personal Data and categories of the Data Subjects and our obligations and rights, and that the Entrusted Parties shall conduct the following matters, must be executed with the Entrusted Parties.

(1) The Entrusted Parties shall process Personal Data only on documented instructions from us, including with regard to transfers of Personal Data to a third country, unless required to do otherwise by the laws of the EU or the laws of the EEA member states to which the Entrusted Parties are subject. If Processing is required by law, the Entrusted Parties shall inform us of that legal requirement before Processing, unless that law prohibits such information on important grounds of public interest;

(2) ensures that persons authorised to process the Personal Data have committed themselves to confidentiality or are under an appropriate obligation of confidentiality;

(3) implement appropriate technical and organisational measures proportionate to the risks required under Article 14;

(4) the Entrusted Parties must inform us about re-entrusting in advance. After obtaining our prior approval on re-entrustment, execute an agreement with the re-entrusted parties, and impose on the re-entrusted parties the obligations relating to data protection that are the same as those in this paragraph, and if the re-entrusted parties fail to perform such obligations, the Entrusted Parties shall be fully liable to us;

(5) taking into account the nature of the Processing, assists us by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of our obligation to respond to requests for exercising the Data Subject's rights laid down in Article 15;

(6) assists us in ensuring compliance with the obligations pursuant to Article 32 to 36 of the GDPR taking into account the nature of the Processing and the information available to the processor;

(7) at our choice, deletes or returns to us all the Personal Data after the Processing of Personal Data by the Entrusted Parties is completed, and deletes existing copies unless the laws of the EU or the laws of the EEA member states require storage of the Personal Data; and

(8) makes available to us all information necessary to demonstrate compliance with the obligations laid down in this paragraph and allows for and contributes to audits, conducted by us or another auditor mandated by us.

Article 11 (Cross-Border Transfer of Personal Data)

11.1 Any transfer of Personal Data to any third party in a third country outside the EEA may take place only in either of the following cases:

(1) where there is an adequacy decision made by the Commission that applies to a third country outside the EEA that will be the transferee; or

(2) where the standard contractual clauses ("**SCC**") adopted by the Commission are contained in an agreement executed by any party to whom a transfer is made, and we have assessed the risks associated with such transfer and taken necessary measures to ensure a level of data protection essentially equivalent to that in the EEA.

11.2 If the transfer specified in the previous paragraph is based on an adequacy decision, then regarding the Processing of Personal Data transferred based on an adequacy decision, we will follow the regulations of the applicable local laws regarding the protection of personal information and the adequacy decision supplementary rules applying to the Processing.

11.3 If the transfer specified in paragraph 1 has relied on SCC, then regarding the Processing of Personal Data transferred based on the SCC, we will perform the obligations under the SCC while following the regulations of the applicable local laws regarding the protection of personal information applying to the Processing.

11.4 Even if none of the items in the preceding paragraph applies, if any one of the following items applies, the transfer of Personal Data to any third party in a third country outside the EEA may take place:

(1) the Data Subject has explicitly consented to the transfer, after having been informed of the possible risks of such transfers for the Data Subject due to the absence of an adequacy decision and SCC;

(2) the transfer is necessary for the performance of a contract between the Data Subject and us or to follow procedures before the execution of a contract at the Data Subject's request;

(3) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the Data Subject between us and a third party;

(4) the transfer is necessary for important reasons of public interest;

(5) the transfer is necessary for the establishment, exercise or defence of legal claims;

(6) the transfer is necessary in order to protect the vital interest of the Data Subject or of other persons, where the Data Subject is physically or legally incapable of giving consent; or

(7) only when the transfer is not repetitive and only a limited number of the Data Subjects, is based on compelling legitimate interests pursued by us (excluding cases where the interests , rights and freedoms of the Data Subject seeking protection of Personal Data outweigh the interests pursued by us), and we have assessed all the circumstances surrounding the data transfer and have on the basis of that assessment provided suitable safeguards with regard to the protection of Personal Data.

11.5 In the case of the transfer of Personal Data to any third party outside the EEA under item (7) of the preceding paragraph we will, as well as notifying the supervisory authority of such

transfer, notify the Data Subject of the transfer and the compelling legitimate interests pursued by us.

Article 12 (Records of Processing Activities)

12.1 We will prepare and maintain records on matters set forth in each item below regarding the Processing of Personal Data:

(1) the name and contact details of ours, the joint controller and the data protection officer (if those have been appointed);

(2) the purposes of the Processing;

(3) a description of the categories of the Data Subjects and the categories of Personal Data;

(4) the categories of recipients to whom the Personal Data have been or will be disclosed;

(5) transfers of Personal Data to a third country (including the identification of the third country), and in the case of transfers referred to in Article 11, paragraph4, item (7), the documentation of suitable safeguards;

(6) envisaged time limits for erasure of Personal Data by category; and

(7) general description of the technical and organisational measures referred to in Article 14, paragraph 1.

12.2 We will prepare and maintain the records referred to in the preceding paragraph in writing.

12.3 We will make the records referred to in paragraph 12.1 available to the supervisory authority on request.

Article 13 (Personal Data Storage Period)

13.1 We will store Personal Data to the extent necessary for the purposes of the Processing.

13.2 We will regularly check if the personal data is necessary in order to achieve the purpose for which it was collected. We will delete data which we determined unnecessary in an appropriate manner. However, the foregoing shall not apply if their safekeeping is legally mandated, or if it is necessary to safekeep in making legal claims or to defend against legal claims.

13.3 We will prepare and maintain an outline of the verification implemented under the preceding paragraph if any.

Article 14 (Technical and Organisational Measures)

14.1 Taking into account the state of the art, the costs of implementation and the nature, scope, context and purpose of Processing Personal Data as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, we will implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk. Upon implementation, it shall be examined whether the following measures may be taken:

(1) the pseudonymisation and encryption of Personal Data;

(2) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of the Processing systems and services;

(3) the ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident; and

(4) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the Processing.

14.2 We will, both at the time of the determination of the means of Processing and at the time of the Processing itself, implement appropriate technical and organisational measures, in an effective manner and to integrate the necessary safeguards into the Processing in order to meet the obligations of the GDPR and protect the rights and freedoms of the Data Subjects. We will regularly evaluate the technical and organisational measures. If necessary, we will implement additional measures.

14.3 Taking into account the matters listed below, we will implement appropriate technical and organisational measures for ensuring that, by default, only Personal Data which are necessary for each specific purpose of the Processing are processed, including ensuring that Personal Data are not made accessible without the individual's intervention to an indefinite number of natural persons.

(1) The amount of Personal Data collected;

(2) the extent of Processing of Personal Data;

(3) the period of storage of Personal Data; and

(4) the accessibility to Personal Data.

14.4 In the case of newly conducting Personal Data Processing activities likely to result in a high risk of infringing the rights and freedom of the Data Subject, as a part of the technical and organisational measures set forth in paragraph 1 above, a Data Protection Impact Assessment pursuant to the GDPR shall be carried out in advance. We shall seek the advice of the data protection officer when carrying out such Data Protection Impact Assessment.

Chapter II Actions to be Taken Regarding the Exercise of Rights by the Data Subject

Article 15 (Exercise of Rights by the Data Subject)

15.1 We will accept the requests listed below by the Data Subject whose Personal Data is processed by us, to the extent permitted by the GDPR:

(1) request for confirmation if his or her Personal Data is being processed, or request for access to his or her Personal Data including requests for copies of her/his Personal Data ;

(2) request for rectification of any inaccurate Personal Data;

(3) request for erasure of his or her Personal Data;

(4) request for restriction of Processing of his or her Personal Data;

(5) request for a right to receive the Personal Data concerning him or her in a structured, commonly used and machine-readable format, or request for transfer to other business operators; and

(6) objection to Processing of his or her Personal Data.

15.2 We may refuse the request from the Data Subject only if her/his identity cannot be verified. Upon acceptance of exercise of rights by the Data Subject under the preceding paragraph, we will duly address them without undue delay (in principle within one month). That period may be extended by two further months where necessary, taking into account the complexity and number of the requests received. We shall inform the Data Subject of any such extension within one month of receipt of the request, together with the reasons for the delay.

Chapter III Action to Be Taken Against Personal Data Breach

Article 16 (Personal Data Breach)

16.1 If there is any potential Personal Data breach (collectively meaning 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; hereinafter the same), we will properly handle it pursuant to this Article.

16.2 In the case of a Personal Data breach, we shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the Personal Data breach to the supervisory authority, unless the Personal Data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.

16.3 If we determine that the Personal Data breach is likely to result in a high risk to the rights and freedoms of the Data Subject, we will notify the Personal Data breach to the Data Subject without undue delay.

16.4 We will prepare and appropriately maintain records of Personal Data breach, if any.

Part III Miscellaneous Provisions

Article 17 (Disciplinary Action)

If a breach of these Rules is found, we will take any action necessary in terms of personnel affairs, including disciplinary action.

Supplementary Provisions

1. Daido Steel Group Europe GmbH shall be responsible for the details, establishment, and revision or abolition of these Rules.

2. These Rules shall be implemented as of 01.12.2022.

3. Date of establishment/revision or abolition
Establishment: 01.12.2022