



Personal Data Protection Policy

Table of contents

1. [Introduction](#)
2. [Terminology](#)
3. [General principles](#)
4. [Purpose of processing](#)
5. [Data subjects's rights](#)
6. [Ensuring the protection of data](#)

Date: 06.07.2023

Rev. 3

This policy applies to Heidelberg Materials Romania S.A.(hereinafter referred to as "**Heidelberg Materials România**" or the "**Company**").

This document may not be reproduced or copied by any third party, in whole or in part, without the written approval of the management of Heidelberg Materials România S.A.

1. INTRODUCTION

This Personal Data Protection Policy has been drafted in virtue of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 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 ("GDPR"), of Law no. 190 of 18 July 2018 on measures for the application of GDPR, of the Guidelines issued by Art. 29 Working Party, namely those issued by the European Data Protection Board. Any regulation (either at European or national level) may trigger the need to amend or supplement this policy.

This Personal Data Protection Policy:

- (i) applies to the **Company's** processing of personal data by electronic means and through classic archiving systems;
- (ii) it does not apply to the obligations that the **Company** may have under national law in its specific field of activity.

THE IMPLEMENTATION AND CORRECT ENFORCEMENT OF THIS PERSONAL DATA PROTECTION POLICY SHALL BE STRICTLY MONITORED BY THE COMPANY.

FAILURE TO COMPLY WITH THIS PERSONAL DATA PROTECTION POLICY MAY LEAD TO SIGNIFICANT FINANCIAL AND REPUTATION LOSSES FOR THE COMPANY AND DISCIPLINARY CONSEQUENCES FOR THE RESPONSIBLE EMPLOYEES.

2. TERMINOLOGY

In this Personal Data Protection Policy, the following terms shall be defined as follows:

"Supervisory Authority"	means the National Supervisory Authority for Personal Data Processing, with headquarters in Bucharest, 28-30 General Gheorghe Magheru Blvd, 1 st District, or any other authority that data protection responsibilities are assigned to under the Legislation for the protection of personal data of any Member state;
"Special Categories of Personal Data"	means Personal Data revealing the ethnic origin, political, religious or philosophical beliefs or membership of trade unions, genetic and biometric data, health related information, sex life or orientation of a natural person;
"National identification number"	means the number that identifies a natural person in certain records systems and which has general application, such as personal identification number, type and number of identity document, passport number, driving license, health insurance number;

"Profiling"	any form of automated processing of Personal Data consisting of the use of Personal Data to evaluate certain personal aspects relating to a natural person, in particular to analyze or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location or movements;
"Personal Data relating to criminal convictions and offences"	means Personal Data relating to criminal convictions, offences and/or pardons;
"Personal Data"	means any information relating to an identified or identifiable natural person and who are protected pursuant to the Legislation for the protection of personal data; for the purpose of this Personal Data Protection Policy, Personal Data include Personal Data relating to criminal convictions and offences and Special Categories of Personal Data;
"Records of processing"	means the records kept by the Company , according to art. 30 of GDPR, providing an overview of all processing activities (e.g. what categories of Personal Data are being processed, by which Organizational Units and what is the purpose of the Processing);
"GDPR"	means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 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;
"Processor"	means an entity processing the Personal Data on behalf of the Controller;
"Legislation for the protection of personal data"	means all the laws and regulations applicable in Romania, whether these represent primary legislation (such as national law and/or GDPR laws) or secondary legislation (such as the Guidelines issued by Art. 29 Working Party/ European Data Protection Board, or other guidelines issued by the Supervisory Authority), applicable for the Processing of Personal Data;
"Controller"	means the entity establishing the purposes and means for processing Personal Data; for reasons related to this policy, the quality of Controller belongs to the Company ;
"Data Subject"	means the identified or identifiable person that the Personal Data is referring to; for reasons related to this Policy, Data Subjects may be employees, customers, representatives of business partners and any other individual whose Personal Data is processed by the Company ;
"Processing"	means 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, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;
"Internal Procedure"	means all the internal procedures, rules, and policies of the Company (regardless of

	their name or subject matter);
"Automated decision-making"	means a process whereby the input data is evaluated solely by IT devices, without involvement from individuals, for example, according to pre-defined criteria/algorithms, the last decision taken having significant consequences for the Data Subject;
"Data Protection Officer" / "DPO"	means an individual designated by the Company pursuant to the Legislation for the protection of personal data; the role of the DPO is to: (a) inform and advise the Company and its employees regarding their obligations of complying with the Data Protection Law; (b) monitor compliance with the Legislation for the protection of personal data; (c) be the contact person for supervisory authorities and individuals whose data are being Processed; details regarding the DPO's rights and responsibilities are provided in this document;
"Subprocessor"	means any person designated by the Processor to process the Personal Data on behalf of the Company ;
"Transfer"	means the disclosure or otherwise making available Personal Data to third parties (including the affiliates of the Company or Subprocessors), either by sending the Personal Data to such third party or by allowing access to such data by other means; storage and back-up shall be considered transfer within the meaning of this Personal Data Protection Policy.
"Organizational Unit"	means, as the case may be, any business line, division, department or internal function of the Company.

3. GENERAL PRINCIPLES

3.1. The Legislation for the protection of personal data requires compliance with the following principles:

<i>Legality, Fairness and Transparency</i>	Personal Data shall be processed in compliance with the law, fairly and transparently in relation to the Data Subject.
<i>Limitation of the Purpose</i>	Personal Data shall only be collected for determined, explicit, and legitimate purposes.
<i>Minimizing the Data</i>	Personal Data shall be appropriate, relevant, and limited to what is required for the purposes for which it is being processed.
<i>Accuracy</i>	Personal data shall be accurate and, when necessary, updated.
<i>Storage Limit</i>	Personal Data shall be retained in a form that allows the identification of Data Subjects for as long as it is necessary to fulfill the purpose for which the Personal Data is being processed.
<i>Integrity and</i>	Personal Data shall be processed in such a way as to ensure them the protection

Confidentiality	against unauthorized or unlawful processing, as well as against accidental loss, destruction or deterioration, and by using appropriate technical, organizational and security measures.
Liability	The Company, acting as Controller, shall be responsible for compliance with the Legislation for the protection of personal data and will have to demonstrate compliance with it.

3.2. The protection of Personal Data is the responsibility of each employee of the Company.

3.3. The Company’s staff shall handle Personal Data with extreme care. The following basic rules are mandatory:

- (i) The **Company** shall process Personal Data for determined purposes; the purpose of Processing has a legal basis;
- (ii) The **Company** is transparent with the Data Subject; the **Company** informs individuals about what it does with Personal Data (regardless of the quality of the Data Subject); the fact that the **Company** obtains the Personal Data of a natural person who is representing a legal person or who is employed by a legal person does not mean that the Personal Data belonging to that person are less important;
- (iii) The **Company** is using Personal Data regarding criminal convictions and offences, only if this is expressly permitted by the legal provision;
- (iv) The **Company** shall make all efforts to ensure that Personal Data is current, complete and accurate, as appropriate, according to the purposes of the Processing;
- (v) The **Company** treats with seriousness any request related to Personal Data, allowing the Data Subjects to correct, delete or restrict the processing of their Personal Data;
- (vi) The **Company** protects your Personal Data against unauthorized losses, changes, disclosures or access.

4. PURPOSES OF PROCESSING

- **The Company holds an inventory with the Purposes of the Processing**
- **The purposes of Processing are exhaustively mentioned in the Records of Processing (kept by the DPO)**
- **Each purpose of Processing has a valid legal basis and is directly related to the Company's activities**
- **The processing of Personal Data should be done in strict compliance with the purposes of Processing**
- **The purposes of Processing are essential for each Processing activity, the DPO being immediately informed of any deviation or amendment thereof**

4.1. Purposes of Processing

4.1.1. In general, the Company processes Personal Data in the following situations:

- (i) when a Data Subject: (a) submits to the **Company** any form, document or information related to its interactions and/or transactions with the **Company**; or (b) uses or

- purchases the **Company's** products; or (iii) concludes a contract (including an employment agreement) with the **Company**;
- (ii) when a Data Subject interacts with the **Company's** personnel, including customer relations officers, technical support officers, or other representatives, for example, by telephone, letters, fax, face-to-face meetings or e-mails;
- (iii) when surveillance cameras capture images with a Data Subject while the latter is found within the **Company's** premises;
- (iv) when the Data Subject asks to be contacted by the **Company**, be included in an e-mail or other mailing lists or when the Data Subject replies to the **Company's** request for the supply of additional Personal Data;
- (v) when a Data Subject interacts with the **Company** using online platforms;
- (vi) when the **Company** acts in order to prevent or investigate suspicion of fraud, illegal activities, omissions or inappropriate behavior regarding the relationship of a Data Subject with the **Company**;
- (vii) when the **Company** complies with or acts upon a request from any public authority or institution or replies to requests for information from them;
- (viii) when the **Company** draws up various reports (e.g. tax, financial, management, risk management and audit);
- (ix) when the **Company** seeks information about a Data Subject or receives the Personal Data of the Data Subject from a third party (for example, from business partners, from the employer of the Data Subject or from public authorities) and uses such data in connection with the relationship between the Data Subject and the **Company**;
- (x) when a Data Subject sends its Personal Data or the Personal Data of a third person (for example, information about its family members and/or employees etc.) to the **Company**, regardless of the reason.

4.1.2. All of the above-mentioned activities are labeled as purposes of Processing and are listed in the Records of Processing.

4.2. Legal Basis of the Processing

4.2.1. The **Company's** purposes of Processing are based on one of the following:

CONSENT	The Data Subject has given his/her consent to the Processing.
PERFORMANCE OF AN AGREEMENT	Processing is required: <ul style="list-style-type: none"> (i) for an agreement that the Data Subject has concluded in his/her own name; or (ii) whereas the Data Subject took any measures prior to the conclusion of an agreement.
FULFILMENT OF A LEGAL OBLIGATION	Processing is necessary as there is a legal obligation on behalf of the Company .
LEGITIMATE INTEREST	The Processing complies with the condition of "legitimate interest".

4.2.2. The legal basis for each of the Purposes of Processing is mentioned in the Records of Processing.

4.3. Minimizing the Personal Data that is being Processed

- 4.3.1. The Purposes of Processing are limited to certain categories of Data Subjects and to certain categories of Personal Data (data minimization).**
- 4.3.2.** The Purposes of Processing refer to Personal Data that is not usually included in the Special Categories of Personal Data nor within the scope of Personal Data relating to criminal convictions and offences.
- 4.3.3.** Processing involving Special Categories of Personal Data should be avoided as much as possible, unless expressly required by law or by the legal provisions or the Internal Procedures.
- 4.3.4.** Furthermore, Processing of Personal Data relating to criminal convictions and offences should be avoided as much as possible, unless it is expressly required by legal provisions.
- 4.3.5.** Any additional Personal Data other than Personal Data specifically mentioned in the Records of Processing and other than the Personal Data mentioned in the Internal Procedures may only be requested from the Data Subjects with prior notice from the Data Protection Officer.
- 4.3.6.** Deliberate or unintentional acquisition of any Personal Data other than the Personal Data specifically mentioned by the **Company** expressly in its Records of Processing and other than those referred to in its Internal Procedures from a source other than the Data Subjects constitutes an event of breach of data security, which needs to be brought to the attention of the Data Protection Officer as soon as possible.

4.4. Accuracy and Confidentiality of Personal Data Processed

- 4.4.1.** All Personal Data collected by the **Company** in connection with any of the purposes of the Processing should be accurate. The **Company's** personnel should ensure that the Personal Data obtained directly or indirectly from Data Subjects is checked, to the extent this is possible.
- 4.4.2.** The integrity and confidentiality of Personal Data Processed are mandatory. The **Company's** personnel shall ensure that the Personal Data acquired directly or indirectly from Data Subjects is safely kept and accessed only for the purposes of Processing, as detailed in the Records of Processing. In this respect, the **Company** shall only provide its personnel with access to Personal Data to the extent that this is necessary for the performance of their job duties.

4.5. Personal Data Storage Limit (Period)

- 4.5.1.** Depending on the purpose of Processing, the Personal Data Processed by the Company shall be kept in a physical and/or electronic format:
 - (i) for the period necessary to accomplish the purpose of Processing; or
 - (ii) for the period provided for by a legal provision; or
 - (iii) for the period necessary taking into account the applicable prescription period.
- 4.5.2.** The **Company** has elaborated and implemented internal archiving rules establishing the period for keeping documents (regardless of their form and title and regardless of whether or not such documents contain Personal Data).
- 4.5.3.** The **Company's** personnel should analyze the Personal Data stored during the work carried out in relation to the internal archiving rules and take the necessary measures to keep or delete the Personal Data in compliance with the applicable legal provisions.

4.6. Changing the Purpose of Processing

- 4.6.1.** In general, Personal Data shall only be Processed for the purposes for which it was initially collected (original purpose). Personal Data may be processed by the **Company** in a manner different from the original purpose (secondary purpose) only if the original and secondary purposes are closely interrelated.
- 4.6.2.** In general, it is permitted to use Personal Data for the following secondary purposes:
- (i) establishing the risk profile of the Data Subject or the company the former represents;
 - (ii) internal audits or investigations;
 - (iii) dispute resolution;
 - (iv) preparing the necessary legal reporting.
- 4.6.3.** Any Processing of Personal Data outside the purposes established under the Records of Processing is prohibited, except for the cases referred to above.
- 4.6.4.** Any change in the purposes of the original Processing shall be carefully assessed in case of doubt by the **Company's** personnel, informing the Data Protection Officer before continuing any further Processing.

4.7. Transfer of Personal Data

- 4.7.1.** In its current activity, the **Company** shall transfer Personal Data to countries outside the European Economic Area or to international/foreign organizations only if the data security is duly guaranteed in that country or international/foreign organization.
- 4.7.2.** When transferring Personal Data to a state outside the European Economic Area, the **Company** shall grant appropriate safeguards for data protection on the basis of an agreement with that natural person, legal person or international/ foreign organization.

4.8. Profiling and Automated Decision-Making

- 4.8.1.** Processing within the **Company** may involve the creation of profiles, automated decision-making or both in the following cases:
- (i) risk management to ensure the security and reliability of the products supplied by the **Company** or in order to prevent and detect fraud;
 - (ii) the creation of profiles of contractors when performing an agreement; this activity may consist in, for example, monitoring the payment history without taking any decision that could affect the contractor's legal situation;
 - (iii) direct marketing;
 - (iv) creating profiles to mitigate the risks that the Data Subject is posing or the circumstances of the contractual partners, if decisions are taken as such.
- 4.8.2.** In all these cases, the **Company** shall observe the rights of the Data Subjects pursuant to the following section.

5. DATA SUBJECTS' RIGHTS

Under the Legislation for the protection of personal data, Data Subjects have specific rights, namely:

- right to be informed;
- right of access;
- right to rectification;
- right to erasure ("right to be forgotten");
- right to restriction of processing;
- right to data portability;
- right to object;
- rights related to decision-making and profiling

5.1. Informing Data Subjects about the Processing Activity

5.1.1. The **Company** shall observe, in all circumstances, the obligation of informing the Data Subjects. The information that needs to be brought to the knowledge of Data Subjects is detailed below:

What information should be provided?	When Personal Data are obtained:
The Company's name and contact details, and the contact details of the DPO, respectively	✓
The Purpose of Processing and the legal basis of the Processing	✓
The legitimate interests of the Company	✓
Categories of Personal Data (when not obtained directly from the Data Subject)	✓
Recipients or categories of recipients of Personal Data;	✓
Details regarding the transfer of Personal Data to third countries and/or international organizations and the security measures related to the transfer	✓
The period that the Personal Data will be stored for and the criteria used to establish such period	✓
The existence of each right of the Data Subject	✓
The Source of Personal Data and whether it comes from public sources	
If the supply of Personal Data represents a legal or contractual requirement, as well as possible consequences of non-compliance	✓
The existence of an automated decision-making process, profiling and information on the decision-making process, its importance and consequences	✓

5.1.2. In the event of Profiling and/or Automated Decision-Making, the **Company** shall ensure the observance of the rights of the Data Subjects:

(i) Obligation to inform - Data Subjects shall be informed, following the commencement of the Processing of Personal Data Processing, about Profiling/Automated Decision-Making, the extent to which Personal Data is involved in the creation of profiles, the logic used

within the method applied and possible consequences of the automated decision-making on the Data Subjects.

When a decision may be pronounced as part of a flow, either in full as a result of an automatic sub-flow or with the intervention of an individual, the Data Subject should be informed of the cases in which the **Company** may take the decision in full by automatic means (as a result of a sub-flow).

When information is being provided regarding the logic that the automated decision-making is based on, it is not required to disclose the algorithm, the formula or the commercial reasoning applied, in detail (such information should not be as detailed as to compromise the **Company's** trade secrets). It is enough to list the Personal Data that the algorithm is taking into account in making the decision and to specify how the data supplied may influence the decision to be taken. The presentation of the way in which automated decision-making is adopted shall be done by using examples.

- (ii) Reviewing the automated decision-making: The Data Subject that undergoes an automated decision-making process has the right to request the involvement of individual on behalf of the **Company** in the decision-making process, to express their point of view and to object to the decision taken in an automated manner. The right to object to automated decision-making does not entitle the Data Subject to request the **Company** to conclude an agreement, but only to oppose the decision based on the automated processing of Personal Data in the event of refusal to conclude the agreement. In any case, the Data Subject needs to be given the opportunity to exercise his/her right to object.
- (iii) right to object: if the legal basis of the Processing is a legitimate interest of the **Company**, the Data Subject has the right to object. In this case, the **Company** should examine whether the opposition is justified (for example, if the interests of the Data Subject exceed the interests of the **Company**) and communicate the decision to the Data Subject.

5.2. Handling the Requests of Data Subjects

- 5.2.1. The Legislation for the protection of personal data requires that any request from a Data Subject shall receive an answer as soon as possible but no later than one month following the receipt thereof. This period may be extended by two months, where necessary, considering the complexity and the number of requests. The **Company** shall inform the Data Subject of any such extension, within one month from having received the request, also specifying the reasons for the delay. Should the Data Subject make a request in electronic format, whenever possible, the information shall be provided in the same format, unless the Data Subject requests a different format.
- 5.2.2. The **Company's** employees shall treat all the requests received from Data Subject about the Processing activity with utmost importance.
- 5.2.3. In all cases, the **Company's** employees shall inform the Data Subjects that they may submit a formal request and/or complaint to the address in Bucharest, District 1, 1A București-Ploiești Road, Bucharest Business Park, Building C2, Floor 1 -4 or to the e-mail address rpd@ro.heidelbergmaterials.com. The **Company** reserves its right to check the identity of the requesting Data Subjects in order to assess the legitimacy of the requests submitted.

6. ENSURING THE PROTECTION OF DATA

6.1. Data Protection Officer

6.1.1. The **Company** has appointed a Data Protection Officer with the qualifications required under the Legislation for the protection of personal data:

- (i) The position of Data Protection Officer is directly subordinated to the President - General Manager of the **Company**;
- (ii) The position of Data Protection Officer is subject to the rules regarding the conflict of interests;
- (iii) The **Company** involves the Data Protection Officer, in due time and in an appropriate manner, in all matters relating to the protection of Personal Data.

6.1.2. In compliance with the provisions of the Legislation for the protection of personal data, the **Company**:

- (i) shall ensure the independence of the Data Protection Officer, who will receive no instructions regarding the performance of his/her duties from any person within the **Company**;
- (ii) shall publish on the website the contact details of the Data Protection Officer to be available to all Data Subjects;
- (iii) shall provide the Supervisory Authority with the name and contact details of the DPO;
- (iv) shall ensure the participation of the DPO in the meetings of the governing bodies of the **Company**, where matters affecting the processing of Personal Data are being discussed;
- (v) shall always give an appropriate weight to the opinion of the DP, and in the event of a misunderstanding, shall document the reasons for not going along with the opinion of the DPO;
- (vi) shall, immediately and without delay, consult the DPO regarding the occurrence of a breach of Personal Data security or other incident;
- (vii) shall support the DPO by providing the necessary resources for the fulfillment of its duties, access to Personal Data and Processing operations, as well as for the maintenance of specialized knowledge thereof;
- (viii) shall provide the regular training of the DPO, who needs to keep abreast of developments in the field of Personal Data protection; The DOP will be encouraged to take part in training courses on the protection of Personal Data and other forms of personal development in order to permanently increase the level of his/her knowledge;

6.1.3. The DPO is required to maintain the secrecy or confidentiality of the information relating to the performance of its duties.

6.2. Internal Duties in order to Ensure the Protection of Data

6.2.1. The compliance with the legal provisions on the Protection of Personal Data is an obligation of each employee of the **Company**, and failure to comply with this policy may entail disciplinary liability.

6.2.2. The **Company** shall provide the human resources and means necessary to implement this Personal Data Protection Policy, including by designating certain individuals within the

Organizational Units, with specific duties in the management of the processes involving the processing of Personal Data, as per the Records of Processing.

6.2.3. These individuals should:

- (i) ensure that the processing of Personal Data is carried out in compliance with this Policy;
- (ii) collaborate with the DPO and implement the changes required to ensure the compliance with the Legislation for the protection of personal data;
- (iii) duly complete and sign the Personal Data Protection Compliance Audit questionnaires and other forms requested by the DPO;
- (iv) perform the impact assessment on the protection of Personal Data and assess the legitimate interest based on the template provided by the DPO;
- (v) obtain the DPO's opinion on all risks or incidents related to the protection of Personal Data, compliance-related issues;
- (vi) submit to DPO reports on the risks related to the protection of Personal Data and compliance-related issues at least once a year or more often, when necessary, or when requested by the DPO;
- (vii) participate, together with the DPO, in investigations or inquiries conducted by a Supervisory Authority in relation to the Processing of Personal Data.

6.3. Internal Procedures

6.3.1. This Personal Data Protection Policy includes the basic principles governing the protection of Personal Data within the Company. All Internal Procedures shall expressly reference this Policy and shall include the express obligation of all employees to comply with its provisions.

6.3.2. The Company shall document the Internal Procedures and shall implement minimum requirements so as to comply with this policy.

6.3.3. In the event of discrepancies between the Personal Data Protection Policy and the Legislation for the protection of personal data, the latter shall prevail.