Principles of Confidential Information Protection and Information Security in KGHM Polska Miedz S.A.

(„Principles")

Version 1.0

The Principles are published at https://kghm.com/pl/przetargi/bezpieczenstwo-informacji. The Principles are an integral part of the agreement („Agreement") concluded by KGHM Polska Miedź S.A. with its registered seat in Lubin („KGHM"), as long as it contains reference to these Principles. The Principles are used to specify the obligations of the entity concluding the Agreement with KGHM („The Contractor"). Hereinafter the Contractor and KGHM will be jointly referred to as the Parties. Whenever a given term is capitalized, the Parties give it the meaning specified in the Agreement, unless the Principles define it differently. By concluding the Agreement, the Contractor confirms that he has read the Principles and undertakes to comply with them.

General Provisions

1. The KGHM has no obligation to disclose Confidential Information. In special circumstances, KGHM may require to fulfil additional requirements and KGHM's internal procedures prior to disclosing this information.
2. Disclosure of Confidential Information does not grant any rights to such information, in particular intellectual property rights, other than the rights expressly set out in a separate Agreement.
3. The Contractor declares that all Confidential Information will be treated as the KGHM's Business Secret and as such are the subject of proper legal protection.
4. The Contractor accepts that KGHM is a public company, the shares of which are listed on the Warsaw Stock Exchange, therefore some information provided under the Agreement may also be confidential pursuant to art. 7 of the Regulation of European Parliament and of the Council no 596/2014 of 16 April 2014 on market abuse (market abuse regulation) and repealing Directive 2003/6/WE of the European Parliament and of the Council and Commission Directives 2003/124/WE, 2003/125/WE and 2004/72/WE (EU Official Journal of 12 June 2014, no. L 173) („MAR Regulation"), therefore, the use, disclosure such confidential information, as well as providing recommendations or inducing another person on the bases of confidential information to purchase or disposal of financial instruments to which such information relates, is subject to liability specified in generally applicable laws, including criminal liability.
5. The Principles also apply to all collective studies, compilations, studies, notes, correspondence and other documents to the extent that they contain any Confidential Information or are based on Confidential Information.
6. The Contractor declares that in the case of processing information concerning KGHM obtained from various sources and compiling it into data bases and performing

operations on these data using IT methods, tools and technologies in order to extract from them new and useful knowledge (so called Big Data), or information will be processed using the so-called artificial intelligence algorithm, any such operation of this type should obtain a prior consent of the KGHM and the results of the above operations regardless of the sources of information used shall be Confidential Information.

7. The Parties agree that the Confidential Information shall be disclosed only to these representatives of the Contractor who, due to the scope of their duties, will be involved in Agreement negotiation and implementation, will be indicated on the list referred to in section 8 below and will sign the Confidentiality Statement in accordance with Appendix No. 1 to the Principles. The Contractor is obliged to expressly inform the persons whom he provides Confidential Information and about the obligations of the Parties resulting from the Principles.
8. The Contractor is obliged to transfer to the KGHM's representatives, mentioned in the Agreement, the list of Contractor's persons entitled to perform the Agreement (in case of any changes such list should be updated). The list mentioned above should be transferred to KGHM at the appropriate time in order to confirm the identity of persons performing the Agreement before starting such activity and should contain: name, surname, business email address and phone number. Update of the list mentioned above may be done only by authorized representatives of the Contractor mentioned in the Agreement. With the list mentioned above, the Contractor shall transfer to KGHM Confidentiality Statement of persons mentioned in point 7 above. The Contractor shall update the statements each time the list is updated. Disclosing of Confidential Information shall be done after transferring complete documentation mentioned above to KGHM.
9. The Parties agree that in the case of the need of disclosing the Confidential Information to third parties (involved in negotiation and realization of the Agreement) by the Contractor – the Confidential Information will be shared with the third parties exclusively:
    a) after informing KGHM about the fact via electronic way and in written form at the latest within 3 days since such need arises;
    b) after receiving a written consent of the KGHM for such a disclosure;
    c) after signing by third party and delivering to the KGHM's representatives set out in the Agreement through the Contractor the Confidentiality Statement in accordance with Appendix No. 1 to the Principles with the list of third parties. To the list, the provisions of point 7 and 8 shall apply mutatis mutandis;
    d) for the responsibility of the Contractor disclosing the Confidential Information to the third party for any breach of the confidentiality obligation resulting from the Agreement.
10. In case of stating or suspecting by the Contractor receiving the Confidential Information that unauthorized disclosure of this information or processing such

information inconsistent with the Agreement or the Principles has occurred, the Contractor shall be obliged to:

a) immediately inform the KGHM about such incident;

b) undertake all possible actions aiming at limiting or removing the effects of the incident;

c) fully cooperate with the KGHM in any actions following incident.

11. The Contractor declare to properly protect the disclosed Confidential Information especially by application of appropriate procedures of processing, organizational security measures and appropriate technical security.

Electronic information processing

1. During performance of the Agreement by the Contractor both Parties may use electronic mail for communication. Both Parties acknowledge, however, that it is not possible to grant safety and faultlessness of electronic data transmission. Such information may be intercepted, defected, lost or damaged. It may reach KGHM or the Contractor with a delay or may be incomplete. It can also be a subject of other unfavourable influences or its use may not be safe. Nevertheless, the Parties are obliged to use adequate safety mechanisms and organizational procedures and communications taking into account the above limitations.
2. The Contractor is responsible for the protection of the Confidential Information regardless its form and the way of its transfer and processing. It means that the Contractor (taking into account the threats accompanying electronic exchange and information processing) is obliged to apply consistent with the current state of knowledge and organizational protections allowing to maintain the required degree of safety.
3. If within the cooperation there is a need of exchanging Confidential Information e.g. by means of electronic mail, each such exchange should be the subject of encryption according to the method agreed upon by the Parties. The requirement of encryption is binding also in the case of exchanging data/information in the form of files using electronic data carriers or transmission via external repositories, data bases or as part of services provided by third parties.
4. The Contractor states that in case of sending, storing or processing the Confidential Information in any other way with the participation of third party, to protect such information encryption methods shall be applied in such a way that the encryption keys will remain at the sole disposition of the Contractor for all the time when the Agreement is binding and the obligations resulting from it exist.

KGHM's information and IT systems access procedures

1. If, as a part of the Agreement, KGHM provides the possibility of access to informatic systems and KGHM's information, such access can be realized by persons involved in the performance of the Agreement, according to scenarios set out below and complying with internal regulations of KGHM.

A. During the performance of the Agreement, warranty obligations or service operations in KGHM's location:

   a. access to information or IT and technical resources for may be provided to particular person subject to prior positive verification of identity,

   b. each time, the Contractor is obliged to agree the scope schedule of works to be performed,

   c. KGHM shall monitor activities of persons mentioned in point a above to check if KGHM's security rules are being respected; during such control KGHM's employee will be present at or supervise activities performed by persons mentioned in the preceding sentence; events registration in the so-called log and session registration shall also be used,

   d. In case of suspected violation of security by persons mentioned in point a above, KGHM is entitled to terminate such persons access immediately,

   e. before completion works performed by persons mentioned in point a. above, if it is possible, appropriate test should be done to confirm data and system integrity,

   f. works performed by persons mentioned in point a above should be completed by signing service performance report.

B. During the performance of the Agreement, warranty obligations or service operations outside KGHM's location:

   a. in order to step up and accelerate the works, KGHM may agree to perform the Agreement by the Contractor with use accepted by KGHM, remote encrypted VPN connection over the internet,

   b. all requirements specified in point A above apply,

   c. upon the Contractor's prior request, KGHM shall provide to persons specified by the Contractor appropriate personal accounts with detailed instruction of making remote connections to KGHM's systems. Persons indicated in the request shall read the instruction for use remote connections and confirm compliance with them,

   d. KGHM is responsible for the proper functioning of the connection, nevertheless inaccessibility of VPN connection shall not be treated by the Contractor as a cause of improper performance or non-performance of the Agreement,

   e. the Contractor is responsible each time for making work arrangements during planned VPN sessions and work schedules,

   f. KGHM, during the works done by the Contractor shall monitor activities of persons mentioned in point c above to check if KGHM's security rules are being respected, During such control KGHM's employee will review system logs, register and verify the course of remote sessions,

   g. In case of suspected violation of security by persons mentioned in point c above, KGHM is entitled to block immediately remote connection. As far

as possible KGHM shall, inform the user of remote connection in direct phone contact about the need to block such session and connection or – in extreme cases – about revoking rights to remote access,

h. persons mentioned in point c above shall inform KGHM's representative by means of the Contractor about the end of using remote connection,

i. each remote session with access to the productive version of system or processing real data may be realized upon prior approval of the KGHM (business owner of the system and information) and agreeing the scope, date and time of the activities to be performed; access permission for remote connections shall be granted only for the time of scheduled activities

j. within the remote user session has a set of functions limited to those that are necessary to perform the operations envisaged; in particular, it is not allowed to connect to the public Internet network and internal KGHM's infrastructure resources at the same time; the above limitations should be taken into account when planning the remote performance of activities provided for in the Agreement.