Information for whistleblowers on the processing of personal data by ComAp a.s. in relation to whistleblowing platform

The company **ComAp a.s.**, with registered office at U Uranie 1612/14a, Prague 7, 170 00, Czech Republic ID no.: 16188667, registered in the Commercial Register maintained by the Municipal Court in Prague under the file no. B 18788 (hereafter "**ComAp a.s.**"), hereby provides you with information on personal data processing in connection with the European Parliament and Council Regulation 2016/679, on the protection of individuals with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC, ("**GDPR**") and Directive 2019/1937/EC on the protection of persons who report breaches of Union law ("**Whistleblowing Directive**").

Please pay attention to the following information, which should provide you with a basic overview of the conditions and scope of the processing of your personal data in connection with ComAp Whistleblowing Policy ("**Whistleblowing Policy**"), in the form of questions and answers. In case you have any additional questions regarding personal data processing, you may contact the Whistleblowing Officer or contact us at privacy@comap-control.com.

1 Who is the controller of your personal data?

1.1 The personal data controller is the company ComAp a.s., with a registered office at U Uranie 1612/14a, Prague 7, 170 00, Czech Republic ID no.: 16188667, registered in the Commercial Register maintained by the Municipal Court in Prague under file no. B 18788, ComAp a.s. is hereafter also referred to as "our company" or "we".

2 On what basis do we process your personal data and for what purposes?

2.1 We need to process your personal data in connection with you reporting a whistleblowing case based on the Whistleblowing Policy and any communication and investigation therewith.

Furthermore, the use of the whistleblowing reporting channels is optional and not using it will not entail any consequences for employees or outside individuals who work on an occasional basis for our company or cooperate with us as suppliers etc.

However, the individual who abuses the reporting channels, (e.g. reports made with malicious intent, to harass or vex, in bad faith, or for personal gain) could face legal consequences. Depending on the jurisdiction, it may result in disciplinary proceedings, penalties, termination of the employment agreement or legal proceedings.

2.2 Your personal data is processed for the purpose of fulfilling our obligations, which includes facts relevant to criminal law, competition law and labor law - Article 6(1)(b) of GDPR, and/or for the purposes of the legitimate interests of the controller – Art. 6 (1)(f) of GDPR.

2.3 Our company does not process your personal data for purposes other than those stated above.

3 What personal data do we process?

3.1 Our company is entitled to process personal data that relate to information that you may have provided in the whistleblowing report, and information we may have acquired over the course of the investigation. Various personal data of various data subjects can be processed, those of whistleblower, individuals mentioned in the report or other documentation acquired during investigation, of witnesses. Any data and information reported are processed solely electronically by an inhouse operated platform.

3.2 It may concern, in particular, the following personal data: academic degrees, name and surname, date and place of birth, job position, contact details, reported facts, elements gathered during the investigation and its outcome.

3.3 There is always a requirement for absolute minimization of the extent of the personal data processed. We process strictly and objectively only data necessary to verify the allegations made.

3.4 Special categories of personal data are not subject to processing, unless they are voluntarily disclosed by you.

4 What are our legitimate interests on personal data processing?

4.1 We have a legitimate interest in the processing to prevent and detect violations and to verify the legality of internal processes and to protect our integrity. Legitimate interest of our company may be deemed to include inter alia the interest on the protection of our property or the interest on the protection of our rights in the event of law suit (right of defense) in accordance with Article 6(1)(f) of GDPR.

4.2 You have the right to object to personal data processing on the basis of legitimate interest at any time.

5 Who and what entities have access to your data?

5.1 Access to your personal data in our company is exclusively granted to authorized person in charge of handling the whistleblowers reports (Whistleblowing Officer). Personal data in the whistleblowing process enjoy special protection and is kept separately from ANY other company data, under permanent security with access only on strictly need to know basis.

5.2 The identity of the whistleblower will be kept confidential at all stages of the process and in particular will not be disclosed to third parties, either to the person against whom the report was directed or to the employee's line management. However, the identity of the whistleblower might need to be disclosed to the relevant people involved in any further investigation or subsequent judicial proceedings initiated as a result of the submitted enquiry. Thus, third parties outside of our company DO NOT have access to your personal data under the whistleblowing process unless it is necessary to provide them to public authorities or advisors (such as law firms) due to the nature of the reported case (criminal offence, legal proceedings).

5.3 Anyone from our company with access to the data in the whistleblowing reporting channels is specifically trained and under reinforced confidentiality obligation.

6 For how long do we process your personal data?

6.1 We store and process your personal data for the entire duration of the investigation and any following proceedings depending on the information reported and how the report is dealt with. Once the case is closed, if the report was classified as inadmissible, we store any information and your personal data for 2 months, otherwise for three (3) years as of the date the report was closed or by the time any period for appeal lapses (including false or slanderous declarations).

6.2 Your personal data is further processed upon the closure of the reported case for the period prescribed by law, in particular for archiving purposes, and for the exercise of our company's legitimate interests (during statutory period limitation if there are any follow-up claims based on the report).

6.3 If any purpose of the processing expires, all of your data or data that served the purpose at hand will be deleted or anonymized, unless there is a reason specified under art. 6.2 above.

7 What rights do you have in relation to personal data processing?

7.1 YOU have the right:

a) to access personal data under art. 15 of GDPR
b) to rectification of incorrect personal data under art. 16 of GDPR
c) to request erasure of your personal data under art. 17 of GDPR
d) to object against the processing under art. 21 of GDPR
e) to withdraw a previously granted consent under art. 13(2c) of GDPR
f) to restricted processing under art. 18 of GDPR
g) to data portability in the extent stipulated by the applicable legislation under art. 20 of GDPR
h) to file a complaint with the Office for Personal Data Protection in case your rights arising from the applicable legislation were violated – for more information see www.uoou.cz.

7.2. If you have any questions or require clarification regarding personal data protection, please contact us at privacy@comap-control.com.

8 Consequences of non-provision of data

8.1 The provision of personal data is carried out on the basis of the legitimate interests of our company. Employees cannot request non-provision and non-processing of such personal data that is necessary for the performance of these obligations during the usage of the whistleblowing system.

9 How are personal data secured?

9.1 The confidentiality of the information provided by using the whistleblowing reporting channels is our top priority. We maintain appropriate technical and organizational measures to ensure data protection and confidentiality and we continually adapt these measures to ongoing technological developments. Among measures are – very limited access, specific training and confidentiality, separated platform and mail server with technological security measures, incident process management. The identity of the whistleblower is revealed only if he/she authorizes it, it is required by subsequent criminal proceedings, or if the whistleblower maliciously makes a false statement. If access is granted to

personal information of a person demanding, any other personal information shall be removed, unless in compliance with previous sentence.

9.2 In case of breach of security of personal data or its misuse, unauthorized disclosure or impairment or compromising thereof, our company will notify the breach without undue delay to the persons, whose personal data has been affected. The notification will include details of the probable consequences of the breach of personal data security and a description of the measures adopted or proposed by our company in order to address the breach of security, including any possible measures to mitigate possible adverse impacts in accordance with company internal processes.

9.3 In the event the breach of personal data security or its misuse results in a high risk to your rights and freedoms, the security incident will be reported to the supervisory authority, which is the Office for Personal Data Protection, based in Prague.

10 Is your personal data being transferred outside your country?

10.1 Our company, located in the EU, is managing the whistleblowing reporting channels for all ComAp branches worldwide. It does not transfer your personal data and does not make it accessible to third parties outside the EU. The company does not intend to transfer this data outside the European Union or the European Economic Area unless it is stated otherwise in a specific case, i.e. the report originally concerns data from non-EU state. With relevant branches we have entered into contractual commitments to ensure that the personal data is kept secure in accordance with applicable law.

11 Contact details for exercising the rights associated with personal data processing

11.1 Any rights, requests or questions concerning the processing of your personal data may be exercised with our company via e-mail at the e-mail address privacy@comap-control.com or in writing to the postal address of the registered office of our company.