Information on the processing of personal data

for new employees
(hereinafter referred to as the "Information")

Art. I
Introductory and general provisions

This Information is published by joint controllers who are parties to, or acceding parties to, the Joint Controller Agreement dated 31 August 2023, which was made in accordance with Art. 26 of the GDPR, in particular:

- MSM GROUP s.r.o., Štúrova 925/27, 018 41 Dubnica nad Váhom, Company Reg. No. *(IČO):* 46 553 509;
- MSM Services, s.r.o., Štúrova 925/27, 018 41 Dubnica nad Váhom, Company Reg. No.: 50 926 748;
- MSM EXPORT, s.r.o., Štúrova 925/27, 018 41 Dubnica nad Váhom, Company Reg. No.: 48 006 122;
- ZVS holding, a.s., Štúrova 925/27, 018 41 Dubnica nad Váhom, Company Reg. No.: 36 305 600;
- ZVS IMPEX, akciová spoločnosť *(joint stock company),* Štúrova 925/27, 018 41 Dubnica nad Váhom, Company Reg. No.: 36 302 848;
- SBS ZVS, s.r.o., Štúrova 1, 018 41 Dubnica nad Váhom, Company Reg. No.: 36 306 070;
- VOP Nováky, a.s., Duklianska 60, 972 71 Nováky, Company Reg. No.: 35 820 322;

(hereinafter individually and collectively referred to as the "Joint Controllers").

The Joint Controllers declare that they process the personal data of data subjects solely for purposes and by means that comply with the requirements of applicable personal data protection legislation, particularly the GDPR (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).

The Joint Controllers have taken security, technical, managerial and organizational measures to ensure appropriate safeguards in accordance with the GDPR. The processing of personal data by the Joint Controllers is therefore lawful, secure, predictable, carried out on legitimate legal grounds and for legitimate purposes, with a sufficient level of protection for the privacy and integrity of the data subject, and the data that the data subject has provided about himself or herself or that is available to the Joint Controllers, in compliance with all processing principles, particularly the principle of data minimization and the principle of storage limitation.

The Joint Controllers have appointed a joint data protection officer (hereinafter referred to as the "Joint DPO"), who will act as a point of contact for any requests from the data subjects and/or third parties, including public authorities. Contact details of the Joint DPO are provided in Art. IV hereof.

The Joint Controllers declare that they do not intend to transfer the personal data they process to a third country, except for data relating to "NSA" (National Security Agreement) issues – as part of this, the personal data of key employees involved in these issues (i.e. not all employees, but only those who are assigned to perform work relating to these issues, undergo relevant training or otherwise come into contact with foreign persons participating in these issues) can be transferred to the USA, to both private legal entities as well as public authorities in the USA in accordance with the NSA. For details see this Information and the Records of Processing Activities (the link is available at the end of this Information), or the Joint Controllers may provide them upon request.

The Joint Controllers do not carry out any automated decision-making or profiling with regard to the personal data and/or data subjects concerned.

Recipients mainly include companies in which MSM GROUP, s.r.o., residing at Štúrova 925/27, 018 41 Dubnica nad Váhom, Company Reg. No.: 46 553 509, has at least a 50% share of voting rights, owns a participation interest, or holds shares representing at least 50% of the registered capital (hereinafter referred to as the "MSM GROUP"), including shareholders and owners of MSM GROUP members. Other recipients may include external advisors and business partners of the Joint Controllers as well as public authorities. No other recipients are envisaged. This statement applies to all processing operations and all purposes for which the personal data are processed, or specifically the "NSA"-related operations and purposes (see above).

Art. II
Personal data processing

The Joint Controllers process the personal data of employees in the following manner and for the following purposes (it is not always possible to determine the period for which the personal data will be stored; therefore, in accordance with Art. 13 (2) (a) of the GDPR, the criteria used to determine that period or the estimated maximum storage period are specified):

1. **Purpose:** **Salary administration**
   Activities included: See the Records of Processing Activities (the link is available at the end of this Information)
   Legal basis: Compliance with a legal obligation / contract performance
   Personal data storage period: Within the meaning of internal regulations of the Joint Controllers, typically for the duration of employment, and subsequently for archiving purposes, for a period of at least 10 years, certain documents for a period of up to 70 years.
   Is it a legal/contractual requirements?: Yes
   Consequences of failure to provide data: Inability to perform the work, loss of employment or non-conclusion of employment contract

2. **Purpose:** **Personnel administration**
   Activities included: See the Records of Processing Activities (the link is available at the end of this Information)
   Legal basis: Legitimate interest / consent / contract performance / compliance with a legal obligation
   Identification of legitimate interest: Recruitment + increasing business efficiency + national security interests + reducing staff turnover + improving employee qualification + ensuring the performance of professional activities + fair remuneration of employees + increasing motivation and work efficiency + communication with employees + improving the work environment
   Personal data storage period: Within the meaning of internal regulations of the Joint Controllers, typically for the duration of employment, and subsequently for archiving purposes, for a period of at least 10 years
   Is it a legal/contractual requirements?: Yes
   Consequences of failure to provide data: Inability to perform the work, loss of employment or non-conclusion of employment contract

3. **Purpose:** **Bookkeeping**
   Activities included: Reporting, including staff performance
   Legal basis: Contract performance
   Personal data storage period: Within the meaning of internal regulations of the Joint Controllers, typically during the evaluation of the relevant period, and subsequently for archiving purposes, for a period of at least 10 years
   Is it a legal/contractual requirements?: Yes
   Consequences of failure to provide data: Inability to perform work properly, inability to calculate remuneration claims and quantitative work indicators

4. **Purpose:** **Management of legal affairs**
   Activities included: Management and recording of legal filings and proceedings, including the protection of legally privileged interests
   Legal basis: Legitimate interest
   Identification of legitimate interest: Protection of legally privileged interests
   Personal data storage period: Within the meaning of internal regulations of the Joint Controllers, typically for the duration of the legal claim, and subsequently for archiving purposes, for a period of at least 10 years
   Is it a legal/contractual requirements?: No
   Consequences of failure to provide data: It is not possible to avoid providing data. Once the employment contract has been entered into and the work performed, the data becomes available to the employer, who can use them to protect their legally privileged interests

5. Purpose: **Marketing and business support**

Activities included: See the Records of Processing Activities (the link is available at the end of this Information), except for the activity of "Addressing potential contractual partners" (this activity does not apply to employees)

Legal basis: Legitimate interest / contract performance / consent / performance of a task carried out in the public interest

Identification of legitimate interest: Business operations + increasing business efficiency + building brand and employee trust + communication with employees + improving the work environment + crisis management + damage/loss prevention and control

Personal data storage period: Within the meaning of internal regulations of the Joint Controllers, typically for the duration of employment, and subsequently for archiving purposes, for a period of at least 10 years

Is it a legal/contractual requirements?: No

Consequences of failure to provide data: Inability of certain employees to perform their work properly, insufficient information about the employer's activities, no entitlement to benefits, inability to present the employer's activities externally

6. Purpose: **Commercial and business operations**

Activities included: Obtaining, maintaining and recording of employee security clearances
Obtaining, maintaining and recording visas for employees

Legal basis: Legitimate interest / contract performance

Identification of legitimate interest: Pursuit of business activities regulated by law + business operations + increasing efficiency

Personal data storage period: Within the meaning of internal regulations of the Joint Controllers, typically for the duration of employment or for as long as necessary to record the relevant documents, and subsequently for archiving purposes, for a period of at least 10 years

Is it a legal/contractual requirements?: No

Consequences of failure to provide data: Inability of certain employees to perform their work properly, threat to the security and legitimate interests of the employer, loss of employment in the worst-case scenario

7. Purpose: **Internal logistics and transport**

Activities included: See the Records of Processing Activities (the link is available at the end of this Information)

Legal basis: Legitimate interest

Identification of legitimate interest: Business operations + increasing business efficiency + building brand and employee trust + communication with employees + pursuit of business activities regulated by law

Personal data storage period: Within the meaning of internal regulations of the Joint Controllers, typically for the duration of employment or relevant entitlement of the employee, and subsequently for archiving purposes, for a period of at least 10 years

Is it a legal/contractual requirements?: No

Consequences of failure to provide data: Inability to make use of the company officers' cars for work/private purposes, inability of certain employees to perform their work properly, inability to order a free vehicle

8. Purpose: **GPS monitoring of vehicles**

Activities included: See the Records of Processing Activities (the link is available at the end of this Information)

Legal basis: Legitimate interest / compliance with a legal obligation

Identification of legitimate interest: Business operations + increasing business efficiency + protection of legally privileged interests + safety + damage/loss prevention + reducing the consequences of accidents + ensuring the performance of professional activities

Personal data storage period: Within the meaning of internal regulations of the Joint Controllers, typically during the use of the company officers' car by the relevant employee, and subsequently for archiving purposes, for a period of at least 10 years

Is it a legal/contractual requirements?: No

Consequences of failure to provide data: Inability to make use of the company officers' car (unless an exception has been granted), reduced ability of the employer to protect the employee from adverse consequences of certain events, loss of control over the location of the vehicle, threat to the employer's legally privileged interests (e.g. as a result of the theft of an unmonitored vehicle)

9. Purpose: Administrative activity

Activities included: Recording and processing of incoming mails
Keeping a work calendar for selected employees
Handling verbal and telephone tasks and messages
Organizing meetings and consultations
Maintaining an employee directory
Records of visitors and persons visited

Legal basis: Legitimate interest/compliance with a legal obligation/contract performance

Identification of legitimate interest: Business operations + protection of legally privileged interests + increasing efficiency

Personal data storage period: Within the meaning of internal regulations of the Joint Controllers, typically for the duration of employment, and subsequently for archiving purposes, for a period of at least 10 years

Is it a legal/contractual requirements?: No

Consequences of failure to provide data: Inability of the employee to perform his or her work properly, potentially the loss of employment

10. Purpose: Compliance with occupational safety requirements

Activities included: See the Records of Processing Activities (the link is available at the end of this Information)

Legal basis: Compliance with a legal obligation / legitimate interest

Identification of legitimate interest: Business operations + increasing business efficiency + safety + damage/loss prevention + reducing the consequences of accidents + protection of legally privileged interests

Personal data storage period: Within the meaning of internal regulations of the Joint Controllers, typically for the duration of employment, and subsequently for archiving purposes, for a period of at least 10 years

Is it a legal/contractual requirements?: Yes

Consequences of failure to provide data: Potential threat to life and/or health, inability to perform work properly, loss of employment

11. Purpose: Ensuring information and physical security

Activities included: See the Records of Processing Activities (the link is available at the end of this Information)

Legal basis: Compliance with a legal obligation / legitimate interest / performance of a task carried out in the public interest

Identification of legitimate interest: Security + damage/loss prevention + protection of legally privileged interests + business operations + increasing efficiency

Personal data storage period: Within the meaning of internal regulations of the Joint Controllers, typically for the duration of employment or consequences of the breach of obligations, and subsequently for archiving purposes, for a period of at least 10 years

Is it a legal/contractual requirement?: Yes

Consequences of failure to provide data: Potential or critical threat to the security of the employer's systems and facilities, inability of the employer to provide employment, bankruptcy, inability to perform work properly, loss of employment

12. Purpose: **Management and control of internal processes**

Activities included: See the Records of Processing Activities (the link is available at the end of this Information)

Legal basis: Legitimate interest / compliance with a legal obligation

Identification of legitimate interest: Business operations + increasing business efficiency + safety + damage/loss prevention + protection of legally privileged interests

Transfer to a third country*: Transfers to the USA, appropriate safeguards are regulated by standard contractual clauses of contracts made between CSG group (a group of companies whose members include the Joint Controllers) and recipients in the USA; for more information, please contact the Joint DPO whose contact details are provided in Art. IV hereof.)

*(*it applies only to a narrow group of employees involved in defined activities within the NSA-related matters)*

Personal data storage period: Within the meaning of internal regulations of the Joint Controllers, typically for the duration of employment, and subsequently for archiving purposes, for a period of at least 10 years

Is it a legal/contractual requirements?: Yes

Consequences of failure to provide data: Inability to perform work properly, loss of employment

13. Purpose: **Personal data protection activities**

Activities included: See the Records of Processing Activities (the link is available at the end of this Information)

Legal basis: Compliance with a legal obligation (GDPR)

Personal data storage period: Within the meaning of internal regulations of the Joint Controllers, typically for the duration of employment or contact with the data subject or existence of legally privileged interests, and subsequently for archiving purposes, for a period of at least 10 years

Is it a legal/contractual requirements?: Yes

Consequences of failure to provide data: Inability to process the necessary data, inability to carry out activities related to the personal data processing, inability to handle a complaint of the data subject

14. Purpose: **Protection of whistle-blowers reporting anti-social activities**

Activities included: Investigating and recording complaints of whistle-blowers

Legal basis: Compliance with a legal obligation

Personal data storage period: Within the meaning of internal regulations of the Joint Controllers, typically when handling a complaint of the whistle-blower or for the duration of related proceedings, and subsequently for archiving purposes, for a period of at least 10 years

Is it a legal/contractual requirements?: Yes

Consequences of failure to provide data: Inability to provide the relevant protection within the meaning of the applicable law, making it more difficult to remedy an unlawful situation

15. Purpose: **Protection of national interests**

Activities included: Prevention activities

Legal basis: Compliance with a legal obligation

Personal data storage period: Within the meaning of internal regulations of the Joint Controllers, typically for the duration of employment or for the duration of potential threat, and subsequently for archiving purposes, for a period of at least 10 years

Is it a legal/contractual requirements?: Yes

Consequences of failure to provide data: The provision of data cannot be refused, when it concerns activities defined by law which must not be jeopardized by failure to provide data

Art. III
Rights of data subjects

The Joint Controllers inform the data subjects of their rights:

1. **Right of access to personal data:** The data subject shall have the right to obtain from the Joint Controllers confirmation as to whether or not personal data concerning him or her are being processed, And where that is the case, access to the personal data and the following information:
   a) the purposes of the processing;
   b) the categories of personal data concerned;
   c) the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations;
   d) where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;
   e) the existence of the right to request from the Joint Controllers rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;
   f) the right to lodge a complaint with a supervisory authority;
   g) where the personal data are not collected from the data subject, any available information as to their source;
   h) the existence of automated decision-making, including profiling - 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;
   i) the right to be informed of the appropriate safeguards relating to the transfer (where personal data are transferred to a third country or to an international organization).

   In this case, the Joint Controllers shall provide the data subject with a copy of the personal data undergoing processing. For any further copies requested by the data subject, the Joint Controllers will charge a reasonable fee based on administrative costs. Where the data subject makes the request by electronic means, and unless otherwise requested by the data subject, the information shall be provided in a commonly used electronic form. The right to obtain a copy shall not adversely affect the rights and freedoms of others.
   The contact point for submitting this type of requests is the Joint DPO (see below for contact details).

2. **Right to rectification of personal data:** The data subject shall have the right to obtain from the Joint Controllers without undue delay the rectification of inaccurate personal data concerning him or her. Taking into account the purposes of the processing, the data subject shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement.
   The contact point for submitting this type of requests is the Joint DPO (see below for contact details).

3. **Right to erasure of personal data ("right to be forgotten"):** The data subject shall have the right to obtain from the Joint Controllers the erasure of personal data concerning him or her without undue delay and the Joint Controllers shall have the obligation to erase personal data without undue delay where one of the following grounds applies:
   a) the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;
   b) the data subject withdraws consent on which the processing is based, and where there is no other legal ground for the processing;
   c) the data subject objects to the processing and there are no overriding legitimate grounds for the processing;
   d) the personal data have been unlawfully processed;
   e) the personal data have to be erased for compliance with a legal obligation under EU or Slovak law, or under the law of another country to which the Joint Controllers are subject;
   f) the personal data have been collected in relation to the offer of information society services.

   Where the Joint Controllers have made the personal data public and are obliged pursuant to the above provisions to erase the personal data, the Joint Controllers, taking account of available technology and the cost of implementation, shall take reasonable steps, including technical measures, to inform controllers which are processing the personal data that the data subject has requested the erasure by such controllers of any links to, or copy or replication of, those personal data.

   The Joint Controllers are not obliged to erase the personal data to the extent that processing is necessary:

a) for exercising the right of freedom of expression and information;
b) for compliance with a legal obligation which requires processing under EU or Slovak law or the law of another country to which the Joint Controllers are subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Joint Controllers;
c) for reasons of public interest in the area of public health in accordance with applicable provisions of the GDPR;
d) for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in so far as the right to erasure of personal data is likely to render impossible or seriously impair the achievement of the objectives of that processing;
e) for the establishment, exercise or defence of legal claims.

The contact point for submitting this type of requests is the Joint DPO (see below for contact details).

4. **Right to restriction of processing:** The data subject shall have the right to obtain from the Joint Controllers restriction of processing where one of the following applies:
   a) the accuracy of the personal data is contested by the data subject, for a period enabling the Joint Controllers to verify the accuracy of the personal data,
   b) the processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead;
   c) the Joint Controllers no longer need the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defence of legal claims;
   d) the data subject has objected to processing pending the verification whether the legitimate grounds of the Joint Controllers override those of the data subject.

   Where processing has been restricted, such personal data shall, with the exception of storage, only be processed with the data subject's consent or for the establishment, exercise or defence of legal claims or for the protection of the rights of another natural or legal person or for reasons of important public interest of the EU or of a Member State. A data subject who has obtained restriction of processing shall be informed by the Joint Controllers before the restriction of processing is lifted.
   The contact point for submitting this type of requests is the Joint DPO (see below for contact details).

5. **Right to object to the processing:** The data subject shall have the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her which is based on the legal ground of "performance of a task carried out in the public interest" or "legitimate interests", including profiling based on these legal grounds. The Joint Controllers shall no longer process the personal data unless they demonstrate compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims. The data subject shall have the right to object at any time to processing for direct marketing purposes, including profiling, to the extent that it is related to such direct marketing – in this case the personal data of the data subject shall no longer be processed for such purposes. Where personal data are processed for scientific or historical research purposes or statistical purposes, the data subject, on grounds relating to his or her particular situation, shall have the right to object to processing of personal data concerning him or her, unless the processing is necessary for the performance of a task carried out for reasons of public interest.
   The contact point for submitting this type of requests is the Joint DPO (see below for contact details).

6. **Right to information about recipients:** The data subject shall have the right to be informed of the recipients of his or her personal data, when requested by the data subject.
   The contact point for submitting this type of requests is the Joint DPO (see below for contact details).

7. **Right to data portability:** The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to the Joint Controllers, in a structured, commonly used and machine-readable format, and the right to transmit those data to another controller without hindrance from the Joint Controllers, where:
   a) the processing is based on consent or on a contract; and
   b) the processing is carried out by automated means.

   In exercising his or her right to data portability, the data subject shall have the right to have the personal data transmitted directly from the Joint Controllers to a new controller, where technically feasible.

   The exercise of the right to data portability shall be without prejudice to the right to erasure ("right to be forgotten"). The right to data portability shall not apply to processing necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Joint Controllers. The right to data portability shall not adversely affect the rights and freedoms of others.

The contact point for submitting this type of requests is the Joint DPO (see below for contact details).

8. **Right to withdraw consent, if personal data are processed based on consent:** The data subject shall have the right to withdraw his or her consent to the processing of his or her personal data based on this legal ground at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal and it shall be as easy to withdraw as to give consent.
The contact point for submitting this type of requests is the Joint DPO (see below for contact details), unless otherwise specified on a case by case basis.

9. **Right to lodge a complaint with the Joint DPO:** If the data subject believes that the processing of his or her personal data infringes the personal data protection legislation, they may complain with the Joint DPO about the procedure followed by the Joint Controllers, in addition to the requests and actions referred to above. The complaint must contain a description of the situation, the reasons why the data subject believes the processing has been incorrect, and their preferred method of remedy. The Joint DPO will handle the complaint and take appropriate actions in collaboration with the Joint Controllers. The right of the data subject to lodge a complaint in accordance with paragraph 10 below shall not be affected thereby.
The contact point for lodging this type of complaints is the Joint DPO (see below for contact details).

10. **Right to lodge a complaint with a supervisory authority:** The data subject shall have the right to lodge a complaint with a public authority that supervises the processing of personal data at any time. Details shall be specified by the responsible authority itself.
The contact point for lodging this type of complaints is the Personal Data Protection Office of the Slovak Republic (*Úrad na ochranu osobných údajov Slovenskej republiky)* (see below for contact details).

Art. IV
Useful contacts and additional information

The contact points for the exercise of rights of the data subject under Art. III hereof are as follows:

Joint DPO:
Address: MSM GROUP s.r.o.
Data Protection Officer
Štúrova 925/27,
018 41 Dubnica nad Váhom
E-mail: osobneudaje@msmholding.sk
Tel.: +421 903 440 747

Supervisory authority:
Address: Úrad na ochranu osobných údajov Slovenskej republiky
Hraničná 12,
820 07 Bratislava 27
Tel. (filing office): +421 2 32 31 32 14
Web: https://dataprotection.gov.sk/sk/

For additional information about the processing of personal data by the Joint Controllers, including all purposes, processing operations, legal bases, proportionality tests and DPIA (Data Protection Impact Assessment), see the Records of Processing Activities available at:
https://www.msm.sk/zaznamy_o_spracovatelskych_cinnostiach (.xlsx format).

By signing below, I confirm that I have read and understood the Information provided.

In ....., dated .....

Name and surname: .....

Signature: .....