JUNE 2024

PRIVACY NOTICE OF PERSONAL DATA PROCESSING FOR DATA SUBJECT – EMPLOYEE
Of U. S. Steel Košice, s.r.o. pursuant to Regulation of the European Parliament and the Council (EU) 2016/

U. S. Steel Košice, s.r.o. pays maximum attention to processing and protection of personal data of its employees, and other data subjects, with emphasis on prevention of unauthorized interference with the privacy of natural persons and the respect for the principles of lawful processing.

The Controller, company U. S. Steel Košice, s.r.o., registered office: Vstupný areál U. S. Steel, 044 54 Košice, Slovak Republic, CRN: 36 199 222, Incorporated in the Companies Register of Municipal Court Košice , Incorporation No.: Sec: Sro, File No. 11711/V (hereinafter the Controller or USSK) processes all personal data in accordance with applicable laws, in particular, with 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) and Act No. 18/2018 Coll. on the protection of personal data, amending certain acts.

In this document data subject – USSK employee, can find all essentials required by Article 13 of GDPR, as well as other required information in relation to processing of your personal data by the USSK. Not all data subjects have their personal data processed for all purposes, it depends on requirements and circumstances or performance content of activities assigned to data subjects and on their work assignment.

1. Processing of personal data – legal basis, purpose and scope

1.1. Legal basis – fulfillment of statutory legal requirement

1.1.1. Specific legal regulations determine the obligation of USSK to process personal data of data subjects and **the processing is necessary in order to fulfill statutory legal requirements of Controller.** In such case, the data subject´s consent is not required, and data subjects shall support such processing of their personal data and provide it for processing. Without the provision of their personal data Controller will not be able to fulfill its statutory requirements, and this could have negative impact on both Controller as well as data subject. Personal data of the employees are also in work documents that are produced as a result of their job description and work position and employer is obliged to have such documents by law, such as job position description or traumatology plan – this data remain in documentation even after employment termination.

1.1.2. **The statutory requirements result mainly** (however not exclusively) from the following legal regulations as amended:

a) Labor Code (Act No. 311/2001 Coll.)
b) Act on occupational safety and health (Act No. 124/2006 Coll.)
c) Act on social insurance (Act No. 461/2003 Coll.)
d) Act on health insurance (Act No. 580/2004 Coll.)
e) Act on Income Tax (Act No. 595/2003 Coll.)
f) Civil Code (Act No. 40/1964 Coll.)
g) Civil Procedure Code (Act No. 160/2015 Coll.)
h) Act on inventions, industrial designs, and improvement proposals (Act No. 527/1990 Coll.)
i) Act on patents (Act No. 435/2001 Coll.)
j) Criminal Code (Act No. 300/2005 Coll.)
k) Offence Code (Act No. 372/1990 Coll.)
l) Administrative procedure (Act No. 71/1967 Coll.)
m) Act on bailiffs and distraints (Act No. 233/1995 Coll.)
n) Commercial Code (Act No. 513/1991 Coll.)
o) Act on Archives and registers and supplementing of some acts (Act No. 395/2002 Coll.)
p) Act on Accounting (Act No. 431/2002 Coll.)
q) Act on Personal data protection (Act No. 18/2018 Coll.)

r) Act on protection of whistleblowers of of Anti-Social Activity (Act No. 54/ 2019 Coll.)
s) Act on reporting of residency of Slovak Republic citizens and citizenship registry (Act No. 496/2002 Coll.)
t) Act No. 315/2016 Coll. on Register of Public Sector Partners
u) Act of economic mobilization and on changes and supplements to Act No. 387/2002 Coll. of governance in crisis situations outside time of war (Act No. 179/2011 Coll.).

1.1.3. **Purposes** of the above presented data processing required by law are mainly:
a) fulfillment of obligations of Controller as employer in relation to labor relations (mainly personnel, wage agenda, trainings and education, administration of recreation allowances);
b) fulfillment of obligations of Controller as employer in relation to observance of duties resulting from regulations on occupational safety and health protection and when providing for the life and health safety and protection including fire safety;
c) investigation of reports and complaints pursuant to Act No. 307/2014 Coll. on certain measures related to reporting of anti-social activity;
d) fulfillment of statutory requirements resulting from accounting or tax regulations;
e) fulfillment of requirements resulting from § 7 paragraph 10 and following of the Act No. 179/2011 Coll. on economic mobilization;
f) fulfillment of statutory requirements in relation to provision of accommodation services;
g) fulfillment of statutory requirements in relation to activities of legal section (mainly the agenda of business companies, preparation of contracts, agenda of licenses and permits, processing and arrangement of compensation for damage to health after occupational injury or occupational illness,
h) fulfillment of obligations pursuant to Act no. 315/2016 Coll. on the register of public sector partners, including the entry of personal data of selected employees - the so-called ultimate beneficial owners to the Register of Public Sector Partners and their publication in this publicly accessible register (including the Internet),
i) Administration of filing department and archive.

1.2. **Legal basis – legitimate interests**

1.2.1. In some cases, USSK goes beyond the strict requirements of the relevant laws or regulation, but only as necessary to pursue protection of our legitimate interests and only in necessary range. These legitimate interests arise from specific activities of our plant, that must fulfill strict security and environmental requirements, as well as requirement to secure safety and health of persons that are present in the USSK. They also come from requirements to comply with selected foreign laws and legal requirements applicable on our mother company residing in U.S.A..
1.2.2. USSK in that case processes personal data necessary for purposes of **legitimate interests** that are pursued by it as Controller or by a third party and for purposes of its protection without the data subject consent. Personal data of the employees are also in work documents that are produced as a result of their job description and work position such as sponsorship of internal documentation – this data remain in documentation even after employment termination.
1.2.3. **The legitimate interests are among others also the following**:
a) providing for the safety, life and health protection, protection of USSK property and material values when entering, moving around and leaving the USSK area and buildings;
b) preparation and issue of personal identification cards for permanent and temporary entries of data subjects on the USSK territory and into USSK buildings;
c) public order and safety protection, criminal conduct detection, detection and documentation of crimes;
d) visual identification of employee (e.g. using of photo and/or video recording);
e) continuous monitoring with camera system namely for the purpose of monitoring of the production technology process, employer property or other entities property protection, life and health protection of persons staying in the public available buildings or in USSK area, observance of occupational safety and health protection rules, investigation of undesirable events, including monitoring of movement of natural persons, prevention and detection of eventual criminal activity;

f) provision of communication and information devices, systems and applications, granting technical support and access rights to applications;
g) administration and organization of social, sports and voluntary events of the company;
h) running the so-called Ethics line;
i) internal audit activities;
j) Compliance agenda, e.g. assessment of eventual Conflicts of interests, assessment of the so-called gifts and entertainment in accordance with valid internal regulations, administration related to arrangement of trainings and education in the ethics and compliance area;
k) control of certain activities of employees, e. g. monitoring of expenses related to printing of documents and phone calls, GPS monitoring of selected company vehicles;
l) compliance with legal obligations outside the EU, including legal obligations binding upon United States Steel Corporation as our mother company;
m) arrangement of court, offense and criminal proceedings (complaints) as well as the establishment, exercise or defense of legal claims;
n) initiating or handling of domestic and cross-border litigations, administrative procedures or investigations (including prevention of destruction of information, their collection, review, analysis and use within such procedures);
o) agenda related to granting loans, recovery of debts from employees and former employees of the company;
p) ensuring network and information security, as well as cyber security (i. e. taking actions to prevent unauthorized access to electronic communication networks and spreading of malicious program codes, as well as stopping the attacks aimed at overloading servers and damage to computer and electronic communication systems;
q) webpage administration including limited number of data when using cookies;
r) creation and maintenance of a database of strengths, knowledge and skills of employees due to their development and effective involvement in new projects, technologies or business opportunities.

1.2.4. Controller can process personal data without the consent of data subject also when processing of personal data appears to be necessary for academic, artistic, literary or journalistic purposes, mainly in relation to company newspaper, respectively similar activity within the corporate social network X-App, social network LinkedIn and platform YouTube.

1.3. **Legal basis – contract fulfillment**

1.3.1. USSK shall also process personal data required for contract fulfillment (especially employment contract), where data subject (employee) is a contract party or following a request of data subject measures shall be taken prior to contract conclusion. Also, in such case USSK as Controller is entitled to obtain personal data directly from employee without his/her consent. Without data provision USSK cannot conclude contractual relation with employee or fulfill its contractual obligations.

1.3.2. Purpose of above presented data processing is mainly:
a) administration of relation with data subject prior to employment or business relation conclusion (the so called pre-contractual relations);
b) performance of selected activities as part of personnel and wage agenda (e. g. social policy and non-wage motivation);
c) in specific cases also preparation of contracts with natural persons is included (e. g. in relation to tangible and intangible assets, deeds of gift, purchase or other contracts) and their internal registration based on requirements resulting from internal company regulations;
d) management of financial support or material gift applications.

1.4. **Legal basis – consent**

1.4.1. If personal data is not processed by means of the methods listed above, USSK can process personal data in exceptional and isolated cases based on voluntarily granted consent of a data subject for purposes specified in the consent, for instance for making or using photographs in some cases. Provision of personal data in the form of consent is voluntary and free.

1.4.2. Data subject can anytime withdraw its consent as of the date of delivery of the written consent withdrawal to the USSK address. Consent withdrawal has no influence on the legality of processing resulting from its consent before the withdrawal.

1.4.3. Old consent that were prepared and expressed in manner and accordance set out in GDPR are remaining valid. Other old consents (including consent in labor contract) expire and are no longer valid and if purpose of processing is still applicable, personal data for these purposes are processed based on other legal basis.

1.4.4. By uploading his photo into Office 365 systems (e.g. Outlook, Teams, etc.), the employee expresses his consent to the processing of his photo by the controller as well as by processors - providers of cloud services and Office 365 systems - by Microsoft. Entering a photo is entirely voluntary.

1.4.5. The controller processes the employee's private e-mail on the basis of consent, or in terms of the agreement on electronic communication (e.g. sending pay slips).

1.4.6. The controller can process personal data that the employee consents to and thus enters about himself within the X-App corporate social network, or LinkedIn, or based on other appropriate legal basis.

1.5. Personal data categories

1.5.1. Processed data fall under, including but not limited to, following personal data categories:

a) **Identification, contact data:** needed for identification the employee within the company's work procedures,registration of entries to USSK property, but also, for example, for the purpose of sorting cleaned work clothes in the laundry, mainly title, name, surname, permanent address, temporary address, correspondence address, date of birth, nationality, type and number of identification card;

b) **Personal agenda data:** data from personal card – name, surname, date of birth, place of birth, nationality, personal identification number;

c) **Data on wages and contribution payments**: data on received and sent payments (especially wages), payment slip related data, data needed for payments of contributions and taxes, attendance record;

d) **Health condition data:** for needs of fulfillment of obligations resulting from legal regulations on occupational safety and health protection, injuries registration and investigation, preventive or occupational medicine, assessment of health fitness of employees, administration of sick leave of employee, etc.;

e) **Operating data on entries** of individual data subjects and on time period spent on the territory and inside buildings of USSK, data on motor vehicle of a natural person – non-entrepreneur;

f) **Photographs and/or camera and/or audio records**;

g) **Data relating to emails, text messages and any other type of electronic communications including traffic data and other personal data contained therein**;

h) **Data on access rights** (e. g. AD account, e-mail address) as well as data recorded during use of information systems and applications (electronic approval, confirmations – log ins, other operations, passwords, user names, etc.);

i) **Other data related to performance of work obligations** (registration of allocated personal protective equipment (self-phone) PPE);

j) **Data contained in the report submitted to the Ethics Line and obtained during the investigation of the report.**

k) **Personal data in documents and records whether in paper or electronic format (**in particular, in agreements, claims, disciplinary documentation, investigative reports, interview notes as well as work documents that are produced as a result of their job description and work position or which an employee is obliged to have by law, such as job position description or traumatology plan).

1.6. Retention period

1.6.1. USSK processes personal data for the processing purpose duration period and for the retention period usually determined by relevant applicable laws and internal regulation – *Registry Order and Registry Plan, Archive and Scholastic Order* or by operational reasons, or entitled interests of Controller.

1.6.2. In case of a litigation, administrative procedure or other investigations, the relevant personal data may be held for the duration of the litigation, procedure or investigation.

1.7. **Data subjects**

1.7.1. Data subjects are mainly:

a) employees of the company USSK;
b) natural persons based on agreements between Controller and Processor (e. g. employees of business companies in which USSK has direct or indirect majority voting rights);
c) other entities based on legal basis set forth by law (e.g. family members, job applicants).

2. Processors /Third parties / Recipients

2.1. Controller has the right (mainly based on written agreement) to delegate a Processor to process personal data of Controller. For the purpose of delegating personal data processing to Processor, the consent of data subject is not required.

2.2. The list of current Processors is available on USSK intranet (including specification of cross-border transfer where applicable) in the section Personal Data Protection, placed on information table located in reception of AB Building, Vstupný areál USSK or upon request it can be provided by Manager Personal data protection process.

2.3. Processors can in specific cases (and after prior consent of Controller) use for service provision the services of a subcontractor and provide personal data to it. If Processor includes into performance of specific processing activities on behalf of Controller another Processor, such Processor is by means of a contract or other legally binding act pursuant to legislation of EU or a member state imposed the same obligations with respect to data protection like the ones specified in a contract or other legal binding act concluded between Controller and Processor, mainly granting sufficient warranties to take appropriate technical and organizational measures in such a way so that the processing meets this Regulation requirements. If such another Processor fails to meet its data protection obligations the original Processor is fully liable to Controller for fulfillment of obligations of such another Processor.

2.4. As Controller, USSK shall not provide personal data to third parties and shall not make them accessible, unless Controller (USSK) is obligated to provide personal data to government authorities pursuant to legal regulations (especially Act No. 315/2016 Z.z. on Register of Public Sector Partners, Social Insurance Act (Act No. 461/2003 Coll.), Health Insurance Act (Act No. 580/2004 Coll.), Income Tax Act (Act No. 595/2003 Coll.), Police Force Act (Act No. 171/1993 Coll.), Act on bailiffs and distraints (Act No. 233/1995 Coll.), Civil Procedure Code (Act No. 99/1963 Coll.) Law on Banks (Act No. 483/2001 Coll.), and others or as otherwise outlined in this document. This category also includes the provision and registration of personal data of selected employees – ultimate beneficial owners to the Register of Public Sector Partners.

A complete extract from the Register of Public Sector Partners can be part of the documentation provided in accordance with the law to other institutions, such as The Commercial Register of the Slovak Republic, public administration and self-government bodies, banks, insurance companies or other institutions, if this is stipulated by law, the said institutions may further process the data from the statement for other purposes. Another purpose may be, in particular, the fulfillment of obligations:

a) established by Act no. 297/2008 Coll. on protection against legalization of income from criminal activity - § 6a) par. 2. establishes the same definition of the ultimate beneficial owner as Act no. 315/2016 Coll. on the register of public sector partners:

b) identification of the client and verification of his identification, which consists, e.g. in requesting personal data of statutory or authorized representatives, copies of identification documents

c) requesting additional information and explanations (for example, ID card number, data from it, etc.).

d) established by Act no. 483/2001 Coll. about banks

e) established by Act 39/2015 Coll. on the insurance industry, while it is valid that in accordance with the aforementioned laws, the USSK is also obliged to provide the bank or other entities with information and documents that are necessary to perform care in relation to the client, or identification and verification of his identification.

2.5. USSK may share personal data with (i) competent EU authorities and jurisdictions in the context of a procedure, an investigation or a request from such authorities and jusrisdictions, (ii) United States Steel Corporation as our mother company (including, where applicable, to enable United States Steel Corporation to comply with a request from competent non-EU authorities and jurisdictions); and (iii) third party service providers and advisors to which USSK and United States Steel Corporation may have recourse, including forensic advisors and consultants.

2.6. In unique cases USSK provides limited scope of personal data also to certain external entities (USSK business partners in relation to fulfillment of business relation or contract) or relevant trade union organization pursuant to provisions of Collective Agreement.

2.7. In specific cases and under the conditions stipulated by relevant legislation USSK also acts as Processor, namely for business companies in which USSK has direct or indirect majority voting rights (daughter companies). USSK performs the following activities for daughter companies - processes the so-called Wage agenda, Personnel agenda, safety – technical services, Compliance agenda and providing of specified IT applications or software or electronic communication networks and systems in order to fulfill work tasks related to labor relation.

3. Cross-border transfer

3.1. When USSK shares personal data with the recipients mentioned above in section 2, it may imply cross-border personal data transfers to countries outside of the European Union whose laws are not considered as ensuring an adequate level of protection, in particular U.S.A. The cross-border personal data transfer can only take place under the requirements and to the scope determined by applicable legal regulations. USSK has procedures in place to ensure that personal data is transferred with appropriate safeguards, such as the Standard Contractual Clauses adopted by the European Commission, or otherwise in accordance with the GDPR, such as if the transfer is necessary for the establishment, exercise or defense of legal claims.

3.2. Some of the specified personal data processing operations are performed by means of applications provided by the company United States Steel Corporation as the mother company of USSK with headquarters in U.S.A., or its subcontractors. When using specified applications, the cross-border transfer of employees´ personal data to U. S. A. takes place. The applications are used mainly to fulfill the work tasks concerning labor relations.

3.3. Also, with respect to global character of the company USSK, some personal data falling under the agenda of human resources, compliance and cybersecurity is transferred and processed by the company United States Steel Corporation as Controller, mainly (but not exclusively) for the following purpose:

a) so called compliance agenda management, namely:

- processing of personal data to provide online trainings (and other training types) and similar or related activities;
- processing and access to data from notifications to the so-called Ethics line and its investigation performed mainly for the reason of protection of entitled interests of USSK and USS;
- processing and access to data acquired and processed by the unit Internal audit;
- compliance with legal obligations outside the EU, including legal obligations binding upon United States Steel Corporation as our mother company;
- arrangement of court, offense and criminal proceedings (complaints) as well as establishment, exercise or defense of legal claims;
- initiating or handling of domestic and cross-border litigations, administrative procedures or investigations (including prevention of destruction of information, their collection, review, analysis and use within such procedures).

b) human resources agenda management (STIP rewards, employees' assessment – Talent management);

c) cybersecurity agenda management (monitoring, detecting, and addressing cyber threats, cybersecurity incident response, administration of Microsoft Office 365 suite).

3.4. USSK may provide you with details on the applicable safeguards and transfers upon request, to the contact details specified below.

4. Data subject rights

4.1. Subject to the conditions outlined in the GDPR, data subjects are entitled to exercise the following rights upon a written request from Controller:

4.1.1. **A confirmation whether** personal data **is being processed** that affects the data subject and if it is the case it is **entitled to access** to the following personal data and information:

a) processing purposes;
b) categories of affected personal data;
c) recipients or categories of recipients to whom personal data was or will be provided, mainly recipients in third countries or international organizations;
d) expected retention period of personal data if possible or, if not, criteria for its specification;
e) existence of the right to ask from Controller the rectification of personal data referring to data subject or its erasing or restriction of processing, or rights to object against such processing;
f) right to file a complaint to supervisory authority;
g) if personal data was not acquired from data subject, any available information as long as its source is concerned;
h) if personal data is transferred to a third country or international organization, data subject is entitled to be informed about appropriate warranties;
i) 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.

4.1.2. **Rectification or supplementing** of its incorrect, incomplete or outdated personal data that is subject of processing, namely by means of supplementary declaration.

4.1.3. **Disposal or erasing** of personal data:

a) that is no longer needed for the purposes for which it was acquired or otherwise processed;
b) that was processed based on a consent if data subject withdraws the consent and there is no other legal basis for its processing;
c) if data subject has objections with respect to processing pursuant to Article 21 paragraph 1 GDPR and no justified reasons for processing prevail or if data subject has objections with respect to processing pursuant to Article 21 paragraph 2 GDPR;
d) if it was processed illegally;
e) if it needs to be deleted in order to meet the statutory requirement pursuant to law of the European Union or a member state to whom Controller is reporting.

This right is not applied if processing is needed: to apply the right for freedom of speech and information; to fulfill statutory requirement that requires processing pursuant to law of the European Union or a member state to whom Controller is reporting or to fulfill a task performed in public interest or when exercising public authority handed over to Controller, for purposes of archiving in public interest, for purposes of scientific or historical research or statistic purposes, to establish, exercise or defend legal claims.

4.1.4. Data subject has the right to ask Controller to **restrict processing** if one of the following cases occur:

a) data subject challenges the accuracy of personal data, namely during the period enabling Controller to verify accuracy of personal data;
b) processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead;
c) the controller no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defense of legal claims;
d) the data subject has objected to processing pursuant to Article 21(1) of GDPR pending the verification whether the legitimate grounds of the controller override those of the data subject.

Controller shall assess the objections listed above pursuant to applicable law.

4.1.5. Data subject has the right to receive the personal data that refer to data subject and that was provided to Controller in structured, commonly used and machine-readable format and has the **right to transfer** this data to another Controller without the Controller to whom this personal data was provided objecting, if:

a) processing is based on the consent or contract and

b) processing is performed by means of automated equipment.

During application of its right for data portability, data subject has the right for personal data transfer directly from one Controller to another one, if it is technically feasible.

4.1.6. Data subject can anytime for reasons referring to its specific situation **object processing of personal data** referring to data subject that is performed based on the legal basis – *fulfillment of task performed in public interest or when exercising a public authority handed over to Controller*; or from a legal reason *the processing becomes necessary for purposes of legitimate interests that are monitored by Controller or third party,* including objecting profiling based on presented provisions. Controller must not further process personal data if it does not prove necessary justified reasons for processing that prevail over interests, rights and freedoms of data subject or reasons to prove, apply or defend legal claims.

4.2. Data subject can claim its right:
a) in written form or electronically and from the content of its claim it shall become obvious that data subject claims its right; and what right is concerned;
b) personally in oral recorded form, whereas from the minutes it shall become obvious who claimed the right, what he asks for, when and who made the record, signature of this person and signature of data subject; Controller shall hand over the copy of minutes to data subject;
c) at Processor's pursuant to letter a) or letter b).

4.3. Data subject can in case of any questions related to personal data protection contact Manager Personal data protection process (the so-called – Personal data protection official or Data Protection Officer pursuant to GDPR) who will answer eventual questions related to processing of your personal data, responsibilities resulting from relevant legal regulations in the area of personal data protection or questions to information contained in this document.
You can contact Personal data protection official using the following contact data:

e-mail address:	dataprotection@sk.uss.com or
written contact:	Manažér procesu ochrany osobných údajov Vstupný areál U. S. Steel 044 54 Košice

In case of any suspicion related to breach of regulations related to personal data protection you can file a notice using the Ethics line of U. S. Steel:

Phone:	+421 55,684 2289
Internet:	www.ussteel.com/corp/EthicsLine
Address:	U. S. Steel Ethics line Vstupný areál U. S. Steel P.O. BOX 17 044 54 Košice

4.4. Data subject can in case of suspicion that its personal data is unlawfully processed file a complaint to the Personal Data Protection Office of the Slovak Republic.

4.5. If data subject is not eligible for legal acts to full extent, its rights can be claimed by a legal representative.

4.6. If data subject does not live, the rights that data subject had pursuant to Act on Personal data protection can be claimed by its relatives.

4.7. Data subjects can ask for identity proof of a person delegated by collection of personal data.