Valoro Consulting Ltd.
Data Management, Data Processing and Data Security Policy

I. Chapter
Introductory Terms

1. Subject of Data Management, Data Processing and Data Security Policy *(hereinafter: Policy)*

1.1. The protection of natural persons in relation to the processing of personal data is a fundamental right.

1.2. In order to ensure a consistent and high level of protection of the personal data of natural persons, Valoro Consulting Ltd. (Registered office: HU-1723 Budapest, Alkotás Street 17-19; Tax number: 24078328-2-43; Represented by: András Holics managing director, hereinafter ***Valoro***), fully respects the legal requirements, ensures the enforcement of the right to informational self-determination, and in particular the constitutional principles of data protection.

1.3. The present Policy defines Valoro's most important responsibilities in relation to the personal data processing and the data security, the rights of data subjects, and the organizational and procedural system of data management.

1.4. In connection with the present Policy, the internal regulations and instructions defining the framework of Valoro's other activities may contain provisions on Valoro's data management and data security activities on an ad hoc basis, but these may not be in conflict with the provisions of the Policy. Should such an event occur, the provisions of the Policy shall prevail until the conflicting rules and instructions are amended.

2. The purpose of the Policy

2.1. With the Policy, Valoro intends to ensure that its data controlling, and data processing activities are carried out within a transparent and regulated framework.

2.2. The Policy serves to comply with the legal provisions governing data controlling and data processing activities, in particular the following legal regulations:

a) 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 (General Data Protection Regulation)

b) CXII of 2011 Act on Informational Self-Determination and Freedom of Information ("Privacy Act")

3. Scope of the Policy

3.1. The subject matter of the Policy extends to all the organizational units of Valoro involved in data controlling and data processing activities, and those persons, and officials which have an employment, assignment, or other work engagement with Valoro.

3.2. The material scope of the Policy extends to all the activities related to the processing of personal data in any IT system or non-IT (paper-based) system which are operated by Valoro.

4. Abbreviations

4.1. The following abbreviations are used in the Policy:

a) *Privacy Act*.: CXII of 2011 Act on Informational Self-Determination and Freedom of Information

b) *Regulation or 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 (General Data Protection Regulation)

c) *Policy:* the present Data Management, Data Processing and Data Security Policy

d) *e-Learning*: a skill development application operated by Valoro

5. Definitions

5.1. For the purposes of the Policy, the following terms shall have the meanings hereunder assigned to them in accordance with applicable law.:

a) *data*: all information in the possession or control of the data controller,

regardless of whether the data is public or confidential, for internal use, restricted or in any way secret or personal data;

b) *data processing*: any operation or set of operations which is performed on personal data or on sets of personal data, whether 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;

c) *controller*: the natural or legal person, public authority, agency, or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;

d) *data deletion*: the complete physical destruction of the data carrier;

e) *data erasure:* making data unrecognizable so that it is no longer possible to recover it;

f) *pseudonymization*: the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organizational measures to ensure that the personal data are not attributed to an identified or identifiable natural person;

g) *biometric data*: the personal data resulting from specific technical processing relating to the physical, physiological or behavioral characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data;

h) *criminal personal data:* all personal data obtained in connection with the criminal offense or the criminal proceedings during or prior to the criminal proceedings, that arise at the prosecuting organizations, the organization of the penitentiary and wich are related to the data subject and/or its criminal record;

i) *recipient:* means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the 4.5.2016 EN Official Journal of the European Union L 119/33 framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing;

j) *data concerning health:* the personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status;

k) *data subject:* any natural person identified or identifiable, directly or indirectly, on the basis of specific personal data;

l) *consent of the data subject*: any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her;

m) *supervisory authority*: an independent public authority which is established by a Member State pursuant to the Article 51 of GDPR, in Hungary the Hungarian National Authority for Data Protection and Freedom of Information;

n) *genetic data*: personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question;

o) *child*: who has not reached the age of eighteen (underage);

p) *third party:* a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data;

q) *special data*: personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership, as well as genetic and biometric data for the unique identification of natural persons, health data and personal data concerning the sexual life or sexual orientation of natural persons;

r) *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;

s) *personal data*: any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

t) *protest:* a statement by the data subject objecting to the processing of his or her personal data and requesting the termination of the processing or the deletion of the processed data.

II. Chapter
Principles

1. Valoro sells organizational development, leadership development and other skills development programs to its customers, as well as online skills development programs. Valoro sells and performs services through subcontractors and employees.
2. While providing the service that is defined in section 1., Valoro processes personal data on behalf of its customers in accordance with the customer's instructions.
3. Valoro performs independent data management for the users of its service when such registration is required for the safe use of online skills development programs, in respect of the personal data that is strictly required for the registration. Valoro may subsequently decide to introduce other data management activities (eg. marketing database, profiling), but this, in all cases, may be based on the customer's consent or other legal basis.
4. To fulfill some of Valoro's services, Valoro uses the services of other data controllers (eg. online questionnaires, surveys). Valoro enters into a data management contract with these data controllers, according to the GDPR.
5. During its data management and data processing activities, Valoro shall respect the following principles for all information relating to an identified or identifiable natural person.
    a) *Lawfulness, fairness, and transparency:* Personal data shall be processed lawfully and fairly and in a way that is transparent to the data subject, thus, it must be transparent to them how the personal data about them is collected, processed, used, and can be accessed. To enforce the principle of transparency, Valoro strives to make its information and communications related to the processing of personal data easily accessible and comprehensible, and to state them in clear and simple language.
    b) *Purpose limitation:* Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.
    c) *Data minimization:* Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed, keeping that in mind that data should only be processed if the purpose of the processing cannot be reasonably achieved by other means.
    d) *Accuracy:* Personal data and the data management shall be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.
    e) *Storage limitation*: Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organizational measures required by the Regulation in order to safeguard the rights and freedoms of the data subject.

f) *Integrity and confidentiality*: Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organizational measures.

III. Chapter
Valoro's data management on behalf of its customers (as a data processor)

1. Valoron - according to its data management and data processing activities - is responsible for the compliance with the above-mentioned principles and must be able to demonstrate such compliance to its customers.
2. Valoro, as a data processor, shall provide its customers adequate guarantees in order to comply with the legal requirements of data processing and to implement appropriate technical and organizational measures to ensure the protection of the rights of data subjects.
3. The data processor may not use an additional data processor without the prior written or general authorization of the data controller (electronic form is also accepted). Due to Valoro's business model, Valoro requests general written authorization from its customers to use an additional data processor (eg. a coaching service provider). Valoro will inform the data controller of any planned changes that involve the use or replacement of additional data processors, thus giving the data controller the opportunity to object to these changes.
4. The processing of data by Valoro shall be governed by a written data processing agreement in accordance with the European Union (hereinafter: EU) law or the law of a Member State, specifying the subject matter, duration, nature and purpose of the processing, the type of personal data, the categories of data subjects and the obligations and rights of the controller.
5. The main elements of the data processing contract concluded by Valoro are:
    a) the subject of the data processing,
    b) the duration of the data processing,
    c) the nature of the data processing,
    d) the purpose of the data processing,
    e) the type of the processed personal data,
    f) the categories of stakeholders,
    g) the obligations and rights of the controller,
    h) personal data required for registration for the safe use of e-Learning (for which Valoro must have a valid purpose and legal basis) only in accordance with the written instructions of the data controller. Including the transfer of personal data to a third country or international organization, unless the processing is required by the applicable EU or Member State law, or Valoro has a different legal consent or other valid legal basis and purpose than which is provided by the customer. In this case, the data processor shall notify the data controller of this legal provision, legal basis, and purpose before the data processing, unless the notification of the data controller is prohibited by the relevant legislation in the important public interest,
    i) Valoro ensures that persons authorized to process personal data are bound by an obligation of confidentiality, or are subject to a duty of confidentiality based on law,
    j) take data security measures that are based on law,
    k) respects the legal conditions for the use of an additional data processor,
    l) assists the controller, taking into account the nature of the processing and taking appropriate technical measures, to fulfill its obligation to respond to requests relating to the exercise of its rights under the applicable law,

m) assists the controller to fulfill its legal obligations, taking into account the nature of the processing and the available information,

n) upon termination of the data processing service, at the discretion of the controller, deletes or returns all personal data to the controller and delete existing copies, unless EU or Member State law requires the storage of personal data,

o) provides the controller all the necessary information to verify the fulfillment of these obligations (provided that this is not restricted by law, contract, official decision or other legal act) and allows and facilitates audits, including on-site inspections, by the controller or another auditor appointed by the controller,

p) Valoro shall immediately inform the controller if it considers that any of its instructions infringe the Regulation or national or EU data protection provisions,

q) if Valoro also uses the services of an additional data processor (based on a contract, or another legal act under EU or Member State law) for specific data processing activities on behalf of the data controller, this additional data processor has to fulfill the same data protection obligations than the obligations which are in the contract between the data controller and processor. The additional data processor must provide adequate guarantees to implement the appropriate technical and organizational measures and ensure that the data processing complies with the requirements of the GDPR. If the additional data controller fails to comply with its data protection obligations, Valoro shall be fully liable to the data controller for the fulfillment of the additional data controller's obligations,

r) other conditions are set out in the model contract annexed to the Policy.

IV. Chapter
Processing of personal data of the natural persons who are not employees

1. The subject of the data

1.1. Data subjects can be divided into several categories, in particular the following:

1.1.1. customers' employees,

1.1.2. e-Learning users.

1.2. Valoro pays special attention to the protection of children's personal data and therefore does not provide services to anyone under the age of 18.

2. The purpose of the data management

2.1. The purpose of data management is the special reason that necessitates the collection, processing and managing of personal data. As the processing of personal data can only take place for a specific, and clear purpose, it is necessary to clearly define the purpose of the data processing before the processing. In case Valoro cannot define the purpose of the data processing, or the customer cannot define the purpose of the data controlling the data processing/controlling shall not take place. At all stages of data management, the purpose of the data management must be appropriate. Once the purpose of the new data processing has been determined, it must be examined whether the purpose of the data processing is lawful in all respects. If the purpose of the data processing is not lawful, the data processing may not take place.

2.2. If Valoro acts as a data processor on behalf of the customer, it must request the customer's written instructions regarding the purpose of the data processing and other legal conditions. If the purpose of the data processing is not lawful, the customer's attention must be drawn in writing to the illegality of the instruction. If the illegal instruction is retained by the customer, Valoro will refuse to process the data.

2.3. The purpose of data processing covered by the Policy (either own data processing or data processing on behalf of a customer) may be, in particular:

a) develop the customer's employees,
b) participation in the customer's assessment team,
c) develop the client's organization,
d) user registration,
e) conducting training and concluding an adult training contract,
f) quality assurance,
g) investigation of a complaint.

3. Personal data that can be managed

3.1. Once the purpose of the data processing has been established, the data to be processed must be precisely and unambiguously defined.

3.2. Once the data has been identified, it is necessary to classify it and determine whether or not it is a personal data. If the data is not a personal data, the provisions of the Policy shall not apply to its processing. In particular, the following are considered as personal data:

- name,
- birth name,
- tax identification number,
- social insurance number,
- birthplace, date of birth
- mother's name,
- permanent address,
- temporary address,
- signature,
- nationality,
- marital status,
- sex,
- age,
- e-mail address (work, private)
- qualifications,
- occupation,
- number of children,
- educational attainment,
- mobile phone number (work, mobile),
- landline phone number (work, mobile),
- position,
- name of employer,
- type of employer,
- personal identification number (personal number),
- ID card number,
- address card number,
- passport number,
- portrait (photo),
- video recording,
- voice (sound) recording,
- created profile,
- IP address.

3.3. If the data is classified as personal data, it must be examined whether the data is

a) a special data,
b) a personal data that can be managed by Valoro.

3.4. It should be noted that certain personal data may not or only exceptionally be processed by Valoro. In particular, personal data - the processing of which is not permitted by law - and which is related to decisions on criminal liability and criminal offenses and related security measures. If the personal data cannot be processed by Valoro, the data may not be processed, and the customer must be informed immediately.

3.5. The processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership, as well as genetic and biometric data for the unique identification of natural persons, health data and personal data concerning the sexual life or sexual orientation of natural persons shall be prohibited. Such data shall be deleted immediately, even if they were provided by the data subject. The customer must be informed immediately.

3.6. In particular, Valoro manages the following personal data:

a) When using online surveys and tests to improve the customer's employees or organization:
    a. data that is necessary for the survey, and usage of tests: name, email address, ("Necessary Survey Data")
    b. profiles and competencies generated on the basis of the evaluation of personality tests ("Survey Results").

b) When participating in the customer's evaluation team: the name of the candidate, the profile that is created during the selection process, the competencies, the results of the selection.

c) c) Registration and other data required for or generated during the use of e-Learning ("Usage Data"). Data required for use: username, email address, login IP address, login time, and so-called local storage ("Required Usage Data") data group is managed by Valoro.

d) d) LXXVII of 2013 Act on Adult Education § 21 (1) and LXXXIX of 2018 Act on Education Register - Valoro, as an adult educator, manages the following in order to conduct training and provide data:

a) the participants'
    aa) data of natural identity,
    ab) education identification number,
b) data related to the training, which is related to the participant's
    ba) education, qualifications and foreign language skills,
    bb) entering and completing training or leaving training without completion,
    bc) assessment and qualification during training,
    bd) payment obligations and the training loan that is used.

4. The legal basis of the data management

Valoro processes personal data only if the processing has a legal basis:

a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes,
b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract,
c) processing is necessary for compliance with a legal obligation to which the controller is subject,

d) processing is necessary in order to protect the vital interests of the data subject or of another natural person,
e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller,
f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

4.1. The consent of the data subject

4.1.1. Valoro processes, in particular, the data below based on the consent of the data subject (own data management):
a) Necessary Survey Data: data that is required to complete the tests and questionnaires used in the Valoro surveys,
b) Survey Results: competency profiles about the data subjects based on the questionnaires and tests,
c) Used Data:the purpose stated by the customer in its own policy for the data subjects (the legal basis is generally the consent of the data subject)
d) Required Usage Data: Enter into a user agreement to use the application and fulfill contract.

4.1.2. Special consent must be requested for Valoro's further processing of contact, registration, and photography data at the end of the development process. In the absence of consent, this data will be deleted. In the absence of consent, the registration will be canceled.

4.1.3. As a data processor, the customer must be required to have the consent to the processing of the following personal data:
a) Photo, creating competency profile,
b) Photo, maintaining a competency profile for more than 6 months,

4.1.4. If the legal basis for the processing is the consent of the data subject, the consent shall be lawful only if the consent is

a) is voluntary, the data subject has a real or free choice, refusing or withdrawing consent without prejudice,
b) clear,
c) specific,
d) based on appropriate information, in particular that its content complies with legal requirements and that its language is comprehensible, clear and simple to the data subject,
e) written (including electronic submission) or oral, or an act that unequivocally expresses consent, in particular if the data subject has made a statement to the customer during the development organized by the customer, when the data subject fills out an online questionnaire, checks the appropriate box when viewing the website, make technical adjustments in connection with the use of information society services and any other action that clearly indicates the data subject's consent to the intended processing of its personal data in that context. Silence, a pre-ticked box, or inaction do not constitute a consent.

4.1.5. The consent shall cover all data processing activities carried out for the same purpose or purposes.

4.1.6. If the data management serves more than one purpose at a time,

a) the consent shall be provided for all data processing purposes,
b) the consent must be provided for each processing purpose, a consent may not cover more than one processing purpose.

4.1.7. If the data subject's consent is given in a written statement relating to other matters, the request for consent shall be made in a manner which is clearly distinguishable from those other matters, in a comprehensible and easily accessible form and in clear and simple language.

4.1.8. If the data subject's consent is given after an electronic request, the request must be clear and concise. It shall not unnecessarily impede the use of the service in respect of which consent is sought.

4.1.9. If the legal basis for the processing is the consent of the data subject, Valoro must be able to verify the existence and lawfulness of the consent. Therefore, Valoro uses a solution that guarantees the lawfulness of the consent, in particular in the case of paper-based data processing the consent is written, while in electronic data processing the service can only be used by those data subjects (users) who sign up electronically.

4.1.10. The data subject has the right to withdraw his or her consent at any time. The withdrawal shall not affect the lawfulness of the data processing before the withdrawal. Valoro will inform the person concerned. Valoro ensures that the consent can be withdrawn by the data subject as simply as it was given.

4.1.11. If the legal basis for data processing is consent, in the case of a child under the age of 18, the processing of children's personal data is lawful only if - and to the extent - the consent has been given or authorized by the person who exercises parental control over the child.

4.1.12. If the legal basis for the processing is the consent of the data subject, the processing of personal data in relation to information society services provided directly to children is lawful if the child has reached the age of 16. In the case of a child under the age of 16, the processing of children's personal data is lawful only if - and to the extent - the consent has been given or authorized by the person exercising parental responsibility over the child.

4.2. Legal obligation

4.2.1. The legal basis for data processing is the fulfillment of a legal obligation of Valoro, if

a) the legal obligation of the data processing is required by EU or Member State law. There is no legal basis if the legal obligation is laid down in a contract.
b) the legal obligation is clear according to the applicable law, it explicitly regulates the nature and object of personal data processing, without giving Valoro an unreasonable discretion with regard to data processing, so that Valoro cannot decide whether or not to fulfill the obligation.

4.2.2. The expediency and professionalism of the legislation is not a condition for the data management that is necessary for the fulfillment of the legal obligation.

4.2.3. Valoro's data management activities cover - in particular - the scope of LXXVII of 2013 Act on Adult Education, 11/2020. (II. 7.) on the implementation of the Adult Education Act, and LXXXIX of 2018 Act on the Education Register, especially for data management under the subheading nr.1. of the education register.

4.3. Performance of the contract

4.3.1. Valoro can also process personal data if processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract.

4.3.2. This legal basis must be interpreted strictly, so that it can only be applied if there is a direct and objective link between the processing and the performance of the contract. The legal basis also covers pre-contractual data processing, pre-contractual relations, provided that this is not initiated by Valoro or by a third party, but by the data subject.

4.3.3. This legal basis shall not be applied if the data processing is not actually necessary for the performance of the contract, in particular if the processing is carried out in connection with the non-performance of the contract or for the purpose of obtaining a direct transaction.

4.4. Legitimate interest, the balancing test of interests

4.4.1. Personal data processing is lawful if it is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

4.4.2. In order to establish the existence of a legitimate interest, it is necessary to carry out a balancing test to examine whether, at the time of and in connection with the collection of personal data, the data subject can reasonably expect that data may be processed. The interests and fundamental rights of the data subject may take precedence over the interests of Valoro if the personal data are processed in circumstances in which the data subjects do not expect further processing.

4.4.3. If the customer invokes its own legitimate interest in its data management instructions in the case of data processing, the customer must be asked to provide the documentation of the balancing test of interest.

4.4.4. The balancing test of interests must be carried out before Valoro starts processing data based on a legitimate interest, in accordance with legal requirements. A sample balancing test of interests is in the Policy. Data processing based on Valoro's legitimate interests may not be initiated if the balancing test of interests has not been established. Valoro will document the conduct of the balancing test of interests and its results in writing, covering all the steps and details of it.

4.4.5. The following steps can be identified in the data privacy process as the steps of the balancing test of interests:

1. step: defining the purpose of data management
2. step: examining the lawfulness of the purpose of data processing
3. step: definition and qualification of the data to be processed
4. step: examination of the legal basis of data processing
5. step: identification of the obstacles to data processing
6. step: determining Valoro's legal interest in data management
7. step: establishing the lawfulness of Valoro's interest
8. step: examining the necessity and inevitability of data management by Valoro
9. step: assessment of Valoro's interest
10. step: assessing the impact of data processing on data subjects
11. step: temporary consideration
12. step: additional guarantees applied by Valoro
13. step: final consideration
14. step: ensuring transparency
15. step: repeating the balancing test

5. Duration of data management

5.1. Personal data may only be processed for the period that is necessary to achieve the purposes of data processing in a way that allows the identification of data subjects.

5.2. Valoro, according to the applicable law, retains personal data in accordance with the various purposes and legal bases of data processing. Then, if it is clear that the data will not be used in the future and the purpose of the data processing has ceased, the data will be deleted or, if possible, anonymised, taking into account the interests of the data subject, the customer and Valoro.

5.3. The retention period may be:

a) 6 months (typical development process duration)

b) in the case of data processing based on the consent of the data subject (pl. e-Learning, online questionnaire) the time until the withdrawal of the consent declaration,

c) after the termination of the contractual relationship between Valoro and the person concerned, until the end of the limitation period (unless otherwise provided by law),

d) in the case of mandatory data management based on legislation, until the expiry of the term prescribed by the relevant legislation (eg. for 5 years in connection with taxation, and for 8 years in connection with accounting)

e) Based on the Section 21 (5) of LXXVII of 2013 Act on Adult Education, Valoro as an adult educator, process the personal data - specified in the IV. Chapter 3.6. d) of the present Policy - until the last day of the eighth year followed by the conclusion of the adult education contract.

5.4. In order to ensure that the storage of personal data is limited to the required time, Valoro sets deadlines for erasure or regular review.

6. 6. Ensuring the enforcement of the data subject's rights

6.1. As a data controller, Valoro enforces the legal rights of data subjects.

6.2. As a data processor, Valoro supports the data controller's customers in fulfilling their obligations to the data controller with regard to the rights involved. Valoro will fulfill the requests within the time specified by law. It does not directly comply with requests for data processed in the course of its data processing activities on behalf of its customers. In such a case, Valoro will refer the data subject to the data controller. But the data controller shall comply with the request for the rights of the data subject without delay, but within a maximum of 5 working days.

6.3. The rights of the data subject:

a) **Right of Information:**
In accordance with the principle of fair and transparent data management, in the case of its own data processing Valoro, or when Valoro acts as a data processor, the customer shall provide the data subject with the information required by law,

b) **Right of Access:**
in the case of its own data processing the data subject - or when Valoro acts as a data processor, the customer according to the data that is processed on its behalf - is entitled to receive feedback from Valoro as to whether the personal data of the data subject is being processed and to have access to the personal data and information required by law. Valoro may charge a reasonable fee based on administrative costs for additional copies requested by the data subject. If the application has been submitted electronically by the data subject or the customer, Valoro will provide the information in a widely used electronic format (eg JSON or .csv), unless otherwise requested by the data subject or the customer.

c) **Right of Rectification:**

in the case of its own data processing the data subject - or when Valoro acts as a data processor, the customer according to the data that is processed on its behalf – shall ask Valoro to correct inaccurate personal data or to supplement incomplete personal data.

d) **Right of Erasure**
In the case of its own data processing the data subject - or when Valoro acts as a data processor, the customer according to the data that is processed on its behalf –, shall ask Valoro to delete the personal data of the data subject (which may be refused only in cases provided by law, in particular if the processing is necessary for the fulfillment of Valoro's obligations to process or enforce personal data, or for the submission, enforcement or defense of legal claims).

e) **the "Right to be Forgotten"**
This right – which is the confirmation of the right of erasure in an online environment - obliges Valoro, in case the personal data should be erased, to take the reasonably foreseeable steps (including technical measures) to inform data controllers that the data subject has requested them to delete links to personal data or the copy of personal data or the personal data itself.

f) **Right to Restriction of Processing**
In the case of its own data processing the data subject - or when Valoro acts as a data processor, the customer according to the data that is processed on its behalf – has the right to have the data processing restricted by Valoro upon request if,

- the data subject disputes the accuracy of the personal data (in this case, the restriction applies to the period that allows Valoro to verify the accuracy of the personal data),
- the processing is unlawful, and the data subject opposes the erasure of the data and instead requests a restriction on their use,
- Valoro no longer needs personal data for data processing purposes, but the data subject requests them in order to make, enforce or protect its legal claims, or
- the data subject has exercised its right to object to the data processing (in this case, the restriction applies for as long as it is established whether Valoro's legitimate reasons take precedence over the data subject's legitimate reasons),

g) **Recipients' Right of Information**
Valoro will inform any recipient to whom or with whom the personal data have been communicated of the rectification, erasure, or restriction of the processing of the personal data. Unless this proves impossible or requires a disproportionate effort. At the request of the data subject or the customer, Valoro will inform the data subject or the customer of these recipients.

h) **Right to Data Portability**
In the case of its own data processing the data subject - or when Valoro acts as a data processor, the customer according to the data that is processed on its behalf –, (when the personal data procession is automatized) is entitled to receive its personal data, which was provided to Valoro (with consent or in connection with the performance of the contract), in a structured, widely used machine-readable format (JSON or .csv) and to transfer the data to another data controller without being hindered by the data controller to whom the personal data have been made available. Or, if this is technically feasible, the data subject may request the direct transfer of personal data between data controllers,

i) **Right to Object**

In the case of its own data processing the data subject - or when Valoro acts as a data processor, the customer according to the data that is processed on its behalf –, is entitled to object at any time, for reasons related to its own situation, to the processing of its personal data necessary for the legitimate interests of Valoro, including profiling. In this case, Valoro and its data controller will not further process the personal data, unless Valoro demonstrates that the processing is justified by compelling legitimate reasons which take precedence over the interests, rights and freedoms of the data subject or which are related to the enforcement of legal claims. If personal data is processed by Valoro for the purpose of direct business acquisition (including profiling), the personal data may no longer be processed for this purpose if the data subject objects. Valoro ensures the data subject - or when Valoro acts as a data processor, the customer, according to the data that is processed on its behalf – to protest at any time, free of charge, against the processing of personal data concerning him for the purpose of direct business acquisition.

j) **The right of the data subject of not being covered by a decision based solely on automated data processing:**

The data subject shall have the right not to be covered by a decision based solely on automated data processing, including profiling, which would have legal effects on him or her would be similarly significant. This right belongs to the data subject in the direction of the customer, as Valoro does not carry out such data processing in its own data management, only on behalf of the customer (eg e-Learning, online questionnaire). This right does not apply to the data subject if

- the making of the decision is allowed by EU or Member State law which is obligatory for Valoro or the customer, and which defines appropriate measures to protect the rights and freedoms and legitimate interests of the data subject,
- the decision is necessary according to the conclusion or the performance of the contract between the data subject and Valoro, or between the data subject and the customer,
- the decision is based on the express consent of the data subject.

In the latter two cases, Valoro ensures the data subject to request human intervention on behalf of the customer, expresses its views and has the opportunity to object to the decision.

k) **Right of Appeal**

If the data subject considers that the processing of personal data violates the legal requirements, the data subject should lodge a complaint for a data protection supervisory authority or have the right to an effective judicial remedy. The data subject has the opportunity to contact Valoro to bring the infringement to an end before submitting the complaint.

7. Content of data management

7.1. Valoro's data management activities include operations on personal data/data files, in particular,

a) collection,
b) recording,
c) systematisation,
d) breakdown,
e) storage,
f) conversion,
g) change,
h) query,
i) insight,
j) use,
k) communication by transmitting, distributing or otherwise making available,
l) coordination,
m) interconnection,
n) the restriction,
o) cancellation,
p) destruction.

7.2. In the event of a restriction on data processing, Valoro will ensure that no further data processing operations are carried out or altered on the personal data. In particular, the personal data in question may be subject to restrictions on data processing

a) for the temporary transfer of a customer to the system,
b) terminating their access to users,
c) temporary removal from the system.

7.3. Real personal data may not be used to verify the correctness of computer and telecommunications equipment and programs, to train users or for educational purposes. In IT (functional, integration) test environments, it must be ensured that the connection between the personal data processed in the live system and the data used and anonymized in the test environment cannot be technically restored. In IT test environments (functional, integration), the use of personal data without anonymization is generally prohibited. Exceptions to this are only possible if testing would not be possible without it. In this case, however, a statement of acceptance of risk from the head of the business area concerned is required. However, the use of personal data should be kept to a minimum and, where possible, replaced with false data or masked, truncated or otherwise anonymized in any way, while ensuring that personal data processed in the live system and used in the test environment (anonymous) data should not be technically re-established as far as possible.

8. Data management by the data processor

8.1. Valoro may use a data processor to carry out its data processing or data controlling activities.

8.2. The data controller - and any person with access to personal data acting under the control of Valoro or the data controller - may process such data only in accordance with Valoro's instructions, unless otherwise required by EU or Member State law.

8.3. Valoro will only use a data processor that provides adequate guarantees to implement appropriate technical and organizational measures to ensure that the data processing complies with legal requirements and that the rights of data subjects are protected.

8.4. The data processing contract of Valoro and its data processor must contain all the conditions that are in the data processing contract between Valoro and the customer. The contract between Valoro and the data processor must include the following:

a) the data processor shall notify Valoro without undue delay
   - if any of the data subject has sought to exercise his right of access, rectification, erasure, restriction of data processing or portability,
   - raises an objection alleging a breach of the legal provisions on data processing.

b) the data processor is obliged to notify Valoro without undue delay if a request concerning the data processing activities of Valoro has been made to it by a data protection supervisory authority or any other authority or court,

c) the data processor shall assist Valoro in fulfilling its obligations regarding the security of data processing, the reporting of the data protection incident to the data protection supervisory authority, the data protection impact assessment and the prior consultation, taking into account the nature of the data processing and the information that is available to the data processor,

d) in the context of assistance, the data processor is obliged in particular on the instructions of Valoro
   - provide information on the processing of personal data to the data subject,
   - provide the data subject with a copy of the personal data which are the subject of the processing, and which are in the possession of the data processor
   - correct or delete personal data.

e) The data processor may not use an additional data processor without the prior written or general authorization of Valoro. In the case of a general written authorization, the data processor shall inform Valor of any planned changes that affect the use or replacement of additional data processors, thus giving Valoro the opportunity to object to these changes.

f) Valoro may withdraw any approval relating to the use of a specific additional data processor (subcontractor).

9. Data transmission

9.1. Personal data processed by Valoro may be transferred within Hungary or to an EEA state only on the basis of one of the legal bases specified in the Policy. The transfer to the EEA State shall be deemed to have taken place in Hungary.

9.2. Personal data may only be transferred or made available to a data controller or processor in a country or in an international organization outside the EEA if:

a) the level of data protection provided by the third country or international organization has been the subject of an adequacy decision by the European Commission, or

b) in the absence of a decision on adequacy under point (a), if the third country controller or processor has provided adequate guarantees, including the provision of an effective remedy for the data subject,

c) the data subject has given its explicit consent to the transfer after being informed of the possible risks arising from the absence of the decision on compliance and appropriate guarantees,

d) the transfer is necessary for the performance of the contract between the data subject and Valoro or for the implementation of pre-contractual measures taken at the request of the data subject,

e) the transfer is necessary for the conclusion or performance of a contract between the controller and another natural or legal person in the interests of the data subject,

f) the transfer of data is necessary in the important public interest,

g) the transfer is necessary for the submission, enforcement, and protection of legal claims,

h) the transfer is necessary to protect the vital interests of the data subject or of another person and the data subject is physically or legally incapable of giving consent,

i) the transmitted data originate from a register which is intended to inform the public in accordance with EU or Member State law and which is accessible for inspection either in general to the public or to any person showing a legitimate interest in it, but only if required by EU or Member State law; the conditions laid down for inspection are met in that case.

9.3. Valoro strives to limit the transfer of data and the amount of data transferred, the possible purposes of its processing and use, the possible duration of its processing, and the possible recipients of the transfer.

9.4. Valoro shall, at the same time as requesting the data transfer, request a statement from the data transferee that the data transferee handles the personal data received to the appropriate extent and in a manner that ensures the data subject's rights in accordance with the data processing restriction. Valoro requires the transferee to undertake that if this becomes important to Valoro for any reason, the transferee will inform Valoro separately about the handling and use of the personal data received.

9.5. The transfer of data, depending on the purpose of the data processing, may take place, inter alia, in the following cases:

a) Outsourcing of all, or part of Valoro's business, providing computer services to Valoro,
b) Valoro's owner, members of the company group to which Valoro belongs, to ensure the flow of data between the group's subsidiaries and interests - in the context of data transfer agreements between those parties - with the consent of the data subject, if necessary, in particular
   - market research,
   - customer satisfaction survey,
   - use for marketing and advertising purposes,
   - ensuring quality and efficient customer service and communication,
c) in order to fulfill the statistical reporting obligation,
d) in the framework of demand management or sales,
e) in order to fulfill the obligation to provide official or judicial information,
f) Valoro's data transmission activities are covered by LXXVII of 2013 Act on Adult Education and 11/2020. (II. 7.) Decree on the implementation of the Adult Education Act.

10. Specific rules on certain data processing

10.1. Website, newsletter

10.1.1. Accessing Valoro's website, e-Learning application and other websites and using the website or the services contained therein, possibly registering on the website or providing or recording data, or using the applications provided by Valoro is limited to that website or possible by accepting the terms of use. By accessing the website or starting to use the application, the website visitor agrees to these terms and conditions and, if necessary, with its active consent.

10.1.2. By accessing the website, if permitted by the visitor's web browser settings or explicitly approved by the visitor on the first visit to the website, the website may automatically save information about the visitor's computer, browsing device (tablet, smartphone) and place computer "cookies", local storages or other similar programs on it. It may only be used for the purpose of preventing abuse and providing the services without interruption.

10.1.3. Computer cookies, local storages, or other similar programs are required to use the application to provide a web experience. (User contract fulfillment is the legal basis.)

10.1.4. 10.1.4. Valoro and the operator of the website record and manage the following data about the visitor, the visitor's computer and the device used for browsing:

a) the IP address used by the visitor, the type of browser, the characteristics of the operating system of the device used to browse (eg. type, language set),
b) the exact date of the visit,
c) the page, sub-page, function, or service used,
d) time spent on the site.

10.1.5. The system automatically logs this data when logging in or out, and the website operator deletes or anonymizes the log files after 6 months.

10.1.6. The data recorded in the system may only be accessed by the employees of the website operator in order to ensure the above purposes.

10.1.7. The transmission of data recorded in the system is only possible in cases specified by law and to authorized persons (typically for law enforcement purposes, etc.).

10.1.8. The anonymised data of the system may be used for statistical reporting purposes.

10.1.9. Valoro may involve a data processor into the operation of the websites. The name of the data processor and the detailed conditions for the data management of the websites and the "cookies" placed on them are contained in the so-called cookies' policy on Valoro's website.

10.1.10. The website also contains links to and from an external server independent of Valoro. The provider of these links may collect user data due to a direct connection to its own server, over which Valoro has no control and assumes no responsibility for such data collection.

10.1.11. Occasionally, Valoro provides services and applications that, with the express and prior consent of users, may also record their personal information for the purposes specified in the terms of use of that service.

10.1.12. Valoro sends regular newsletters to its customers. A natural person who registers for the newsletter service on the website may consent to the processing of its personal data by checking the appropriate box. It is forbidden to check the box in advance. The data subject may unsubscribe from the newsletter at any time by using the unsubscribe application of the newsletter, or by making a written or e-mail statement, which means the withdrawal of consent. In this case, all data of the subscriber must be deleted immediately.

10.1.13. The personal data used for the newsletter is the name and e-mail address of the natural person. The legal basis for data processing is the consent of the data subject. The period of storage of personal data lasts until the existence of the newsletter service, or until the data subject's consent is revoked or deleted.

10.1.14. The purpose of processing personal data is to send newsletter about Valoro's services.

IV. Chapter
Processing of personal data of the representatives of non-natural persons

1. The Policy

   a) is not applicable to the processing of data of non-natural persons,
   b) is applicable to the processing of personal data of the following natural persons: representatives, proxies, owners (hereinafter together: **representatives**) of those persons that are defined in point a).

2. Valoro may, in particular, process the following personal data concerning the representatives.

3. The purpose of the processing of representative's personal data is in particular:
   a) identification of the representative of the non-natural person, prevention of possible misuse of identity documents, investigation of possible misuse,
   b) ensuring contact with the representative,
   c) performance of the contract concluded with a non-natural person, provision of the service undertaken under the contract, verification and inspection of the obligations and rights related to the contract, communication and provision of information related to the contract,
   d) asserting, collecting and selling any claims that may arise in connection with the contract;

4. In addition to the representative's consent, the source of the processed data may be a public and authentic register (such as, in particular, the company register or other similar register).

5. Valoro shall process the personal data of the representative for the same period as the data of the represented non-natural person.

V. Chapter
Processing of personal data of natural persons who are employees

1. Scope of the present Chapter

This chapter applies to the processing of employees' personal data by Valoro as an employer. The other chapters of the Policy mutatis mutandis apply to the processing of personal data of employees. Pursuant to this chapter, the rules applicable to an employee shall also apply to a natural person's trustee or trainee employed in a legal relationship for personal work.

2. Purpose of the personal data processing

1. The purpose of the data processing covered by this chapter is to ensure that the employment complies with the rules of labor law, as well as with the principles of employment and work, both during and before its existence.

2. The purpose of the data processing covered by the Policy is also to enable Valoro as an employer to exercise its rights, enforce and protect its legitimate interests, fulfill its legal and contractual obligations, perform labor, payroll and social security administration tasks, measure employee performance, do human resource management, recruitment, careers, and do the administration of benefits.

3. The purpose of data processing based on legislation is to fulfill the obligations and exercise the rights contained in the given legislation. The data processing prescribed by law is considered to be mandatory data processing, the extent and duration of which are determined in each case by the relevant legislation.

4. Valoro, as an employer, informs the employees about the data processors who process their personal data. Valoro informs employees in separate internal instructions about the details, rights and obligations associated with the statutory data processing, and the data processing when Valoro is an employer.

5. Data processing based on non-specific legal data processing obligations is at the discretion of Valoro (as an employer) and may serve the following purposes:

    a) examination of the suitability of potential employees - candidates, candidates sought during the selection - in order to select the appropriate workforce,

    b) to facilitate selection informing previous candidates about new job opportunities, and vacancies at the Valoro,

c) in order to maintain the employment, the evaluation and qualification of the employee, the design of its job in an appropriate manner, the examination of the employee's suitability,

d) control of work and employee behavior, thereby protecting Valoro's (as an employer) financial, economic and ownership interests,

e) fulfillment of obligations prescribed by law after the termination of employment, enforcement of any claims.

6. In all cases of non-statutory data processing, Valoro (as an employer) acts in accordance with the purpose limitation principle. This ensures that the processing can only take place for a pre-determined, lawful and fair purpose, only to the extent and period that is required, and in the presence of an appropriate legal basis.

3. Legal basis of the personal data processing

1. It may be the legal basis for employment-related data processing
   a) the consent of the data subject,
   b) a provision of law,
   c) the protection of the legitimate interests of the controller or of a third party.

2. The data subject's consent can only be a legal basis for data processing in connection with the establishment or termination of the employment, not for data processing during the employment.

4. Processed personal data of employees

1. As an employer, Valoro only asks its employees to make a statement or disclose information and thus process personal information that
   a) does not infringe the employee's personal or data protection rights,
   b) is relevant to the establishment, performance or termination of the employment, which is directly related to the purpose of the employment,
   c) which is prescribed by law (labor law, social insurance, tax law, employment protection or other similar rules related to employment) or which is necessary for the exercise of a right or obligation specified in the law.

2. As an employer, Valoro manages, in particular, the following personal data about its employees in connection with their employment:
   a) personal identification data,
   b) contact details,
   c) data on education, qualifications, further training / education, examinations and their completion and assessment,
   d) data on family, relatives, marital status,
   e) work-related fitness and health data,
   f) data related to previous work, especially information on previous jobs, jobs,
   g) data related to social insurance, taxation, payroll accounting,
   h) data related to conflicts of interest and other suitability related to the filling of the position,
   i) data generated in connection with the performance of work - such as data generated in connection with the evaluation, qualification and performance of the employee's work.

3. In some cases, such as conflicts of interest, certain benefits and subsidies, Valoro, as an employer, also handles the personal data of the employee's relatives.

5. Usage and acquaintance of the employee's personal data

1. As an employer, Valoro may only disclose facts, data, opinions or other information about an employee to a third party in cases specified by law or with the employee's express consent, failing which it will not transfer or transfer personal data to such persons.

2. According to the law, personal data may be transferred to, for example, the investigating authority, the public prosecutor's office or a court, the tax authority, the social security, pension and health insurance authority, the health insurance fund or, in the case of registrants, the court of registration.

3. Personal data processed by Valoro as an employer about an employee may be disclosed to other employees of Valoro as an employer only if and to the extent strictly necessary for the performance of their duties. The personal data thus disclosed are the responsibility of these employees.

4. In order to fulfill its obligations arising from the employment relationship, Valoro, as an employer, may transfer the employee's personal data to a data processor or subject them to joint data processing, provided that the purpose of the data provision and other conditions specified by law are complied with.

5. Data relating to an employee may be used for statistical purposes or may be provided in an anonymized manner without such consent.

6. The duration of the processing of employee data is determined taking into account the provisions of the current labor, tax and social security legislation.

6. Data management related to the establishment of an employment relationship

1. Prior to the establishment of the employment, the purpose of the data management is to enable the employment to be established in the interests of Valoro (as an employer) and the potential employee. To this end, only personal data that may contain relevant information about the data subject's suitability shall be processed prior to the establishment of the employment.
2. Valoro, as an employer, retains the data of the applicants until a decision is made to establish the employment.
3. As an employer, Valoro may carry out a suitability test for each job and decide on the results.
4. If the data show that an employment relationship cannot be established in the future, Valoro, as the employer, will delete the data immediately, unless the employee specifically requests further processing of the data for the purpose of establishing a later employment. In the latter case, Valoro, as the employer, may process the employee's data until the consent is withdrawn and may only transfer the employee's data to a third party for this purpose with the employee's consent. The data subject may at any time request the deletion of its personal data or withdraw its consent, which Valoro, as the employer, will comply with. Valoro, as the employer, informs all those to whom the employee's data has been transferred for the purpose of data processing.
5. Valoro, as an employer, deletes personal data - without request - in applications which were sent for the purpose of establishing an employment, if the data clearly show that an employment cannot be established in the future.
6. As an employer, Valoro may process the personal data necessary to make a decision on the

employment prior to the establishment of the employment. And those that are needed to create an employment, and to conclude an employment contract.

7. The legal basis for Valoro's data processing mentioned in this section is the prior consent of the data subjects, the fulfillment of a legal obligation or the legitimate interest of Valoro as an employer.

7. Suitability for the job

1. The examination of the employee's medical fitness is always carried out by an occupational health doctor in accordance with the applicable legislation. Valoro, as an employer, only receives information about the employee's suitability, otherwise it does not process the employee's health data.

2. Valoro, as an employer, reserves the right to examine the suitability of an employee for certain positions and to prescribe specific suitability tests for this purpose.

3. As an employer, Valoro reserves the right to require a specific skills test or a mandatory psychological assessment for certain jobs. A condition assessment will only be carried out if the nature of the job clearly justifies it. Principles of psychological assessment (test):

   a) the test shall be carried out only if there is a clear justification for the post in question,
   b) the test may be carried out only by a suitably qualified professional,
   c) about the purpose, method and possible consequences of the test Valoro, as an employer, informs the employee,
   d) Valoro, as an employer, is informed of the results of the test to the extent justified and necessary,
   e) Valoro, as the employer, ensures that the employee is not disadvantaged during the test and the management of the result,
   f) Valoro, as an employer, treats the data generated in connection with the test as confidential, particularly protected data and ensures that it is not disclosed to unauthorized persons. As an employer, Valoro sets up its control system so that as few people as possible have access to the data. Valoro, as an employer, concludes contracts with those persons requiring appropriate confidentiality,
   g) the persons concerned are provided with detailed information on the psychological assessment before the start of the assessment.

4. If the job justifies it or is required by law, Valoro, as the employer, will call on the employee to obtain its judicial record and hand it over to Valoro as the employer. Valoro, as the employer, keeps the judicial record together with other documents relating to the employee, in compliance with data security requirements.

8. Data on qualifications

1. Valoro, as an employer, keeps all data on the employee's education and qualification which are related to the employee's job and employment. Valoro, as an employer, keeps other kind of data on education and qualification based on the employee's information.

2. As an employer, Valoro has the right to make copies of documents certifying qualifications and education.

3. Valoro, as an employer, has the right to contact the relevant educational institutions in order to verify the authenticity of the documents certifying the qualification and education, and to request information, and to process the data obtained during the verification.

4. The employee is obliged to inform Valoro as an employer about the acquisition of additional qualifications related to the work.

5. As an employer, Valoro has the right to request information from the employee about studies under a study contract with the employee. If the employee participates in the training at the discretion and expense of Valoro as an employer, Valoro may become aware of the data related to the training, and the employee is obliged to provide information about these.

9. Inspection of the working rules

1. As an employer, Valoro has the right to monitor the compliance with the rules of employment and to carry out data processing to this end.

2. The purpose of the inspections is to prevent and detect acts that are illegal and detrimental to Valoro's interests, and to ensure that the employees use Valoro’s assets in accordance with their intended purpose.

3. During the inspection, personal data will only be processed in accordance with the principles of the relevant legislation and the Policy, as well as other applicable regulations, with the knowledge of the data subject. The employee has the right to know the purpose and course of the inspection and the related data management. As an employer, Valoro provides an opportunity for the person concerned to express his or her views before the inspection.

4. During the inspection activity and data management, Valoro, as an employer, is obliged to respect the employee's personal rights and reputation, and to apply the least intrusive inspection method possible.

5. Valoro, as an employer, reserves the right to keep the data files separated in the event of a suspected criminal offense and to make them available for the authorities in official or criminal proceedings.

6. According to the applicable law Valoro may transmit the data and evidence of the illegal acts to the competent authority.

10. Inspection of the ability to work

1. Valoro, as an employer, reserves the right to check the employee's fitness and ability to work, which may include checking for non-alcoholic status. The inspection can be carried out primarily if it is probable that the person concerned is intoxicated on the basis of external signs - appearance, behavior, communication. The inspection must not be aimed at harassing an employee.

2. The above-mentioned rule also applies to the control of the intoxicated person (eg. under the influence of drugs). However, such an examination may be carried out only by an authorized specialist with the consent of the employee. If the employee's intoxicated condition is reasonably suspected, Valoro, as an employer, may file a report of a drug abuse offense with the competent investigative authority.

11. Inspection of the post mails

1. An employee may not engage in private correspondence at its workplace address. The employee must do everything to ensure that its private letters do not reach Valoro's address as an employer.

2. Consignments received on behalf of the employee must be handled in accordance with the general records management rules. If it is clear that the letter is private, it must be forwarded to the employee concerned. Letters delivered in this way, if they are official, must be returned by the employee to the general filing process.

3. Opened, private letters must be forwarded to the recipient, and Valoro may not know or use their contents. Valoro may require the employee not to pursue private correspondence at work. In the event of the opening of a private letter, the employee must be informed of the identity of the person opening the letter.

12. Inspection of the electronic mails

1. Due to the fact that electronic mailing is available on Valoro's means and servers, employees may not use their work email addresses for private correspondence.

2. As an employer, Valoro has the right to check outbound correspondence on its IT devices and the electronic mail addresses of Valoro. If the inspection reveals that the outgoing letter is private, Valoro may carry out the inspection with due regard for privacy.

3. Incoming e-mails may be checked only in exceptional cases. If necessary, Valoro, as the employer, provides the employee with the option to delete incoming private mail in the presence of Valoro’s representative (as the employer) or save it to an uncontrolled location on its own data carrier. If the incoming letters are for private purposes and contain personal data, the employee must delete them immediately so that personal data cannot become the property of Valoro as an employer during any inspection.

4. Electronic mail can be checked in justified cases, primarily in order to prevent and detect abuses.

5. During the inspection, Valoro strives to ensure that its knowledge of private secrets is kept to a minimum. If the inspection involves private secrecy, Valoro is obliged to ensure the presence of the employee during the inspection and to draw the employee's attention to this.

6. As an employer, Valoro has the right to restrict correspondence to work email addresses, both the content and the scope, and any of the attachments, by incorporating automatic filters to ensure that emails of a certain size, or with certain attachments, files are prevented from being sent or received. This can be done primarily for IT security purposes.

7. If Valoro, as the employer, archives the contents of the electronic mailbox, the employee is obliged to delete any private correspondence prior to archiving. Valoro, as the employer, is obliged to draw the employee's attention to this in advance.

8. If an employee is impeded (particularly, but not exclusively, due to illness, leave) and it is assumed that an important e-mail related to Valoro’s activities has been received in the

employee’s electronic mailbox, the employee may authorize another employee to access the mailbox. If the employee does not authorize anyone to do so, the employee’s superior shall have the right to access, only to the letters relating to the purpose of the access, for the duration of the obstruction.

9. In the event of termination of employment or in case of the absence of the employee (especially, but not limited to, sickness, maternity leave), Valoro, as the employer, has the right to copy the contents of the employee's e-mail account and make it available for one or more other employees to ensure business continuity.

10. All employees are required to cancel any private correspondence prior to termination of employment.

13. Inspection of the work phones’ use

1. Valoro, as the employer, reserves the right to monitor the use of telephones to the extent and for the purposes set out in the Policy, and to contact the telecommunications service provider to provide a detailed call list.

2. As the employer, Valoro reserves the right to control the outgoing calls of all work phones, the duration of the calls, the number called, and the cost of the call. The employee makes a call from the work phone knowing that Valoro, as the employer, has access to its data.

14. Use of the Internet

1. As Internet access is available at Valoro's expense and on Valoro's devices and may only be used for work purposes, Valoro may monitor employees' use of the Internet to the extent necessary for the purposes set forth in this Policy. In doing so, Valoro can learn what websites the employee is viewing and what they are downloading from and uploading to. The employee uses the Internet in the knowledge that Valoro, as an employer, may have access to the data of the visited pages visited.

2. Valoro, as the employer, exercises its right to access in order to prevent and detect illegal acts and those that harm Valoro's business interests.

3. As the employer, Valoro reserves the right to restrict or prohibit access to certain websites and types of websites and to download or upload certain files, file types and content. As an employer, Valoro also has the right to restrict or prohibit access to websites that provide certain services, such as mail systems, social networking sites, and online stores. As the employer, Valoro informs employees of its decision. Valoro is entitled to take the necessary organizational and technical measures to implement the decision.

15. Inspection of the use of IT tools

1. Valoro, as the employer, is the owner of the IT assets of the workplace and the data stored on the devices. As the employer, Valoro reserves the right to inspect the data carriers of the workplace. Employee must refrain from storing private content on the IT devices of the workplace.

2. As the employer, Valoro reserves the right to make modifications to IT devices of the workplace that prevent the insertion, connection, and access to external media.

3. As the employer, Valoro is not obliged to allow the insertion and connection of external data carriers and access to networks on newly acquired IT equipment.

16. Data management related to the entry control system

1. As the employer, Valoro has an electronic entry control system.
2. Valoro uses an electric entry system to control the entry and exit of employees. It also aims to protect property, identify the people entering the headquarters, control access and stay, and prevent unauthorized entry.
3. To use the entry control system, Valoro provides an identification card to all employees that allows them to pass through the gates belonging to the access control system.
4. During the use of the entry system, the personal data of the cardholder, the card ID, the place, time, and direction of transit will be recorded. Data recorded during the use of the entry control system will be deleted after 30 days unless the use of the data is necessary in a labor dispute between Valoro as an employer and the employee.
5. Valoro, as the employer, uses the data generated in the entry control system to detect and eliminate situations that directly threaten the security of persons and property, and to detect acts that violate them.
6. Data generated in the entry control system are available to security professionals and those who involved in labor disputes.

17. Monitoring the observance of working hours

1. Valoro, as the employer, is entitled to process data in order to monitor the observance of working hours.
2. The data obtained during the inspection may be used to prosecute for the detected illegal practice or to take other action.
3. As the employer, Valoro informs the employees concerned about the details of the data processing, the rights and obligations related to it.

18. Conflict of interest check

Valoro manages the data according to the conflict-of-interest regulations to determine whether the employee's additional employments and interests are compatible with the employment with Valoro and do not infringe on Valoro's rights or legitimate interests.

19. Internal abuse reporting system

As the employer, Valoro operates an internal abuse reporting system to prevent and detect abuse. In this connection, Valoro, as the employer, manages only the necessary personal data with respect of the data subjects' rights.

20. Managing data on prohibiting legal consequences

As the employer, Valoro keeps in the employee's personal records the information on the prohibiting legal consequences that were used in connection with the employee.

21. Data management in connection with trade union membership and works councils

1. The processing of personal data referring to trade union membership is prohibited. This data can only be processed in cases defined by law, in particular if
    a) the data subject has given his explicit consent to the processing of the data for one or more specific purposes,
    b) the processing is necessary to fulfil the obligations of Valoro as an employer, or obligations of the data subject which is arising from the legal provisions and social protection system,
    c) data processing is in the legitimate activities of a trade union foundation, association or any other non-profit organization, provided that the processing relates exclusively to members of such an organization or persons who are in regular contact with the organization and that personal data are not made available to persons outside the organization without the consent of the data subjects.

2. At the written request of the employee, Valoro deducts the union or other interest representation membership fee from the employee's salary. Valoro is obliged to transfer the amount specified in the request to the union until the termination of the mandate.

3. Valoro, as the employer, manages the data on the employee's trade union membership if the trade union membership fee is deducted from the employee's salary.

4. Valoro, as the employer, manages the data on the positions of the employees of Valoro's trade union and works council in order to record the benefits, rights and obligations related to the position.

22. System of personal records, preservation of documents

1. As an employer, Valoro ensures that the manner and content of personnel records always comply with applicable law. Statutory data processing is mandatory and may be requested by data subjects.

2. The personnel register is structured in order to separate the data processing according to the legal basis and purpose. By setting up a system of personal records, defining entitlements and taking organizational measures Valoro, as the employer, ensures that the information contained in the personnel register is accessible only to those employees who need it in order to perform their duties.

3. Valoro provides access to personnel records, according to data security requirements, to those data processors who provide Valoro a service related to the management of personnel matters.

4. As the employer, Valoro may make copies of certain employee documents that contain personal information to verify the accuracy of the information.

5. Valoro, as an employer, stores and keeps paper-based documents in the personnel records in accordance with data security requirements.

6. As the employer, Valoro operates the electronic records in a way that is compliant with the data security requirements.

23. Data management related to the terminated employment

1. In connection with the termination of employment, only the certificates required by the Labor Code will be prepared. A different evaluation and qualification of the work of the data subject is possible only at the express request of the data subject.

2. After the termination of employment, personal data may be stored in accordance with the provisions of the legislation or on the basis of another appropriate legal basis. If the statutory period of data processing has elapsed or the purpose of the data processing has ceased, the data will be deleted.

3. Valoro, as the employer, reserves the right to process any data that may be required in a subsequent dispute until the expiry of any existing claims arising out of or in connection with the employment.

4. The employee's e-mail account will be deleted after termination of employment, unless it becomes necessary to copy the e-mail box after deleting any private e-mails to ensure continuity of employment. If, as a result of the employee's job, it is presumed that the e-mail address receives letters related to Valoro's activities as an employer, Valoro as an employer is entitled to maintain the mailbox for a predetermined period of time. As an employer, Valoro may examine incoming mail, but is required to delete private mail. Mail cannot be sent from the mailbox.

5. After the termination of the employment, Valoro, as the employer, may examine postal mails that are addressed to the employee, but private letters shall be sent to the addressee if possible.

VI. Chapter
Data protection organization

1. Data protection organization

1.1. The following operators are involved in the management and performance of data protection activities:
   a) the manager
   b) the data protection coordinator
   c) IT manager,

1.2. The manager
   a) issues Valoro's Privacy, Data Processing and Data Security Policy,
   b) appoints the Valoro’s data protection coordinator.

2. The data protection coordinator

2.1. Valoro employs a data protection coordinator.

2.2. Valoro ensures that the data protection coordinator is involved in all matters - in an appropriate time - relating to the protection of personal data in an appropriate manner. In particular, Valoro requires the data protection coordinator to provide professional advice when carrying out a data protection impact assessment.

2.3. Valoro supports the data protection coordinator in the performance of its duties, by providing the resources that are needed to carry out these tasks, access personal data and data management operations, and maintain the data protection coordinator's expertise.

2.4. Valoro ensures the independence of the data protection coordinator.

2.5. Valoro may not dismiss or sanction the data protection coordinator in the performance of its duties.

2.6. The data protection coordinator is directly accountable to Valoro's top management.

2.7. Data subjects may contact the data protection coordinator in all matters relating to the processing of their personal data and the exercise of their rights.

2.8. the data protection coordinator is bound by the obligation of confidentiality specified in EU or Hungarian law in connection with the performance of its duties.

2.9. The data protection coordinator may perform other tasks, provided that Valoro ensures that no conflict of interest arises from these tasks.

2.10. The data protection coordinator shall perform, inter alia, the following tasks:

a) provide information and professional advice to Valoro, its customers and data processing staff on their obligations under EU or national data protection rules;
b) monitor compliance with EU or Member State data protection provisions and Valoro's internal rules on the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in data processing operations, and related audits;
c) provide professional advice on data protection impact assessments upon request and monitor the conduct of impact assessments;
d) cooperate with the supervisory authority,
e) to act as a contact point for the supervisory authority in matters relating to data processing, including prior consultation, and to consult with it on any other matter as appropriate;
f) notify the supervisory authority of the data protection incident.

2.11. The data protection coordinator shall perform its duties with due regard to the risks associated with the data processing operations, taking into account the nature, scope, circumstances and purpose of the data processing..

2.12. The data and information requested by the data protection coordinator shall be provided to the data protection coordinator within the time limits and in the manner specified by the data protection coordinator.

2.13. Contact of the data protection coordinator: info@valoro.hu.

VII. Chapter
Data protection procedure

1. Data protection impact assessment

1. If any type of data processing to be carried out by Valoro (given its nature, scope, circumstances and purposes) is likely to pose a high risk to the rights and freedoms of individuals, Valoro will carry out an impact assessment prior to the processing to ensure how involved the intended data processing operations are. Similar types of data processing operations with similar high risks can be assessed in a single impact assessment.

2. The data protection impact assessment should be carried out in particular in the following cases:
    a) a systematic and extensive assessment of certain personal characteristics of natural persons, based on automated data processing (including profiling) and on which decisions having legal effect on the natural person or a significant effect on the natural person are based,
    b) the processing of special categories of personal data,
    c) large-scale, systematic monitoring of public places,
    d) there is a systematic analysis or evaluation of workers' performance, reliability, and behavior at work, in particular by automated means,
    e) introduction of a video surveillance system or change of the applied technology,
    f) introduction of new, innovative technological solutions (eg. cloud services, AI technology, e-Learning, use of questionnaires).

3. The impact assessment shall cover at least the following:
    a) a systematic description of the planned data processing operations and a description of the purposes of the data processing, including, where applicable, the legitimate interest that Valoro intends to pursue,
    b) an examination of the necessity and proportionality of the data processing operations in the light of the purposes of the data processing,
    c) to examine the risks to the rights and freedoms of the data subject,
    d) the demonstration of risk management measures, including safeguards, security measures and mechanisms to protect personal data and demonstrate compliance with legal requirements, taking into account the rights and legitimate interests of data subjects and others.

3. Procedure to be followed in respect of the data subject 's requests

1. If the data subject or the customer contacts Valoro in connection with the exercise of the data subject's rights, in particular if the data subject requests information about the data processed by Valoro, requests a copy thereof, requests the correction or deletion of data processed by Valoro, restricts data processing, or exercise its right to data portability, the data subject's application must be forwarded to the data protection coordinator without delay.

2. the data protection coordinator shall examine the application and notification without delay,

if necessary, with the involvement of the organizational unit concerned.

3. If the data subject's request cannot be complied with, the data protection coordinator shall reject the request and inform the data subject within one month of the filing date of the request.

4. If the data subject's request can be complied with, the data protection coordinator shall inform him or her within one month of the filing date of the request. It shall take the necessary measures to comply with the request and shall inform the person concerned of the measures taken.

4. Obligation of documentation

1. Valoro must be able to demonstrate compliance with the principles governing the processing of personal data. Compliance shall be demonstrated, in particular, by appropriate documentation of the circumstances and decisions on which the data management decisions are based, the information and statements made to the data subject and the statements made by the data subject.

2. Valoro records and stores information on all activities and decisions related to data management in a documentable and retrievable form.

3. If the data processing is carried out on the basis of a legitimate interest after the balance of interests has been carried out, Valoro shall record and store the findings, results and other documentation of the balance of interests in writing in a documentable and retrievable form.

4. If data management takes place after an impact assessment has been carried out, Valoro will record and store the findings, results and other documentation of the impact assessment in writing, in a documentable and retrievable form.

5. If the data is processed with the consent of the data subject, Valoro will record and store the consent statement (in writing, online, via electronic message, video chat and otherwise) in a documentable and retrievable form. If the consent was given orally, by telephone, Valoro shall record the statement made by the data subject in this way by means of a sound recording, and shall record and store the recorded sound recording in a documentable and retrievable form. Valoro records the data management information provided to the data subjects and its content in a documentable and retrievable form.

5. Register of personal data

1. Valoro ensures that the manner and content of the registration of personal data complies with the legislation in force at any time.

2. Valoro ensures proper, logical and necessary physical separation of data processing for different purposes and for different customers.

3. Valoro manages electronic and paper-based records according to uniform principles, taking into account the characteristics of the media in the records. The principles and obligations under the Policy apply to both electronic and paper-based records.

4. Valoro ensures – with the definition of rights and other organizational measures - that the information contained in the records is accessible only to those employees and those acting in the interests of Valoro / the client who need it in order to perform their duties through the structure of the register system.

5. Valoro provides access to the register to data processors who provide Valoro a service related to data processing.

6. Valoro's electronic records comply with data security requirements and ensure that only those who need them to access their data have access to them for a specific purpose.

6. Register of data management activities

1. Valoro shall keep written records (including in electronic format) of the data processing activities for which it is responsible. Valoro may also use a special application for this record.

2. The register of data management activities shall contain the following information:
   a) the name and contact details of Valoro,
   b) if any, the name and contact details of the data controller,
   c) that Valoro treats the personal data in question as a data controller or processor,
   d) the name and contact details of the Valoro representative,
   e) the contact details of the Valoro data protection coordinator.
   f) the purposes of the data processing,
   g) a description of the categories of data subjects,
   h) a description of the categories of personal data,
   i) the categories of recipients to whom the personal data will or will be communicated, including recipients in third countries or international organizations,
   j) where applicable, information on the transfer of personal data to a third country or international organization, including the identification of the third country or international organization and, in the case of a transfer, a description of the appropriate guarantees,
   k) where possible, the time limits for deleting the different categories of data,
   l) a general description of the technical and organizational measures to ensure a level of data security commensurate with the degree of risk to the rights and freedoms of natural persons.

3. Valoro shall make the register available to the supervisory authority upon request.

7. Termination of data management, deletion and destruction of personal data

1. If the purpose of Valoro's data processing has been achieved, the processed data is no longer required by Valoro or the customer on the customer's instructions, the processing of the personal data must be erased, deleted or destroyed.

2. The method of storing the data in an IT manner shall be chosen in such a way that it can be erased at the end of the erasure period or, if necessary for other reasons, taking into account the possible erasure period. Personal data must be erased in such a way that the data can no longer be identified and can be recovered, and the erasure is irreversible and verifiable.

3. Paper-based media must be deprived of personal data with the help of a shredder or a professional shredding person. Rules for the disposal of electronic data carriers in the case of electronic data carriers are used (hard disks, optical data carriers, magnetic data carriers, printers, storage media for multifunction machines, flash (NAND) data carriers, SIM cards, mobile devices, telephones, PDAs, laptops, etc.), physical destruction and, if necessary, prior secure and irrevocable erasure of the data must be ensured. The destruction of data carriers must be checked and documented, and the documentation must be retrieved or disposed of in a retrievable manner in accordance with the provisions of the relevant regulations.

4. The obligation to delete data cannot be fulfilled by pseudonymisation itself, as pseudonymous personal data can later be linked to a natural person using additional information and should therefore be considered as data relating to an identifiable natural person.

5. With the physical data deletion, the obligation of data deletion is fulfilled. This is when the data is physically deleted, the record is actually deleted or the data to be deleted is physically overwritten (eg by entering the "X" characters in the appropriate field).

6. Logical erasure of data is acceptable if the solution effectively ensures the non-recognition of personal data and the prevention of re-use.

7. The deletion method, which cannot even be considered as a logical deletion, is not acceptable, the deleted data is dimmed but clearly legible on the interface, and the data is still in the IT system, it still exists in the database in a visible, recognizable form - with this technique of deletion the data management is not eliminated.

VIII. Chapter
Data security, data protection incident, customer audit

1. Data security

1. In its data controlling and processing activities, Valoro shall keep in mind that personal data must be managed in a way that ensures an adequate level of security and confidentiality, including in order to prevent unauthorized access to personal data and the means used to process personal data. or their unauthorized use.

2. Valoro ensures the security of the personal data that it manages.

3. In order to ensure data security, Valoro will take the necessary technical and organizational measures for both data files stored on IT media and those stored on traditional paper-based method.

4. Valoro shall take appropriate technical and organizational measures - while take into account the state of science and technology and the costs of implementation, as well as the nature, scope, circumstances and purposes of data processing and the varying likelihood and severity of risks to the rights and freedoms of natural persons - to guarantee a level of data security commensurate with the level of risk. These measures may include, in particular:
    a) the pseudonymization and encryption of personal data,
    b) ensuring the continued confidentiality, integrity, availability and resilience of the systems and services used to process personal data,
    c) in the event of a physical or technical incident, the ability to restore access to and availability of personal data in a timely manner,
    d) a procedure for the regular testing, evaluation of the effectiveness of the technical and organizational measures taken to ensure the security of data processing.

5. In determining the action to be taken, Valoro shall explicitly take into account the risks arising from the processing of personal data, in particular from the accidental or unlawful destruction, loss, alteration, unauthorized disclosure or unauthorized disclosure of personal data transmitted, stored or otherwise managed.

6. Valoro shall take measures to oblige persons with access under its control to process the data in accordance with the purpose limitation principle in accordance with Valoro's instructions, unless they are required to do so by EU or Member State law.

7. Valoro shall take the necessary measures to ensure that access to the data is restricted to those who need it in order to carry out their duties according to the purpose limitation principle.

8. Valoro ensures the enforcement of data security rules through separate regulations, instructions, and procedures. It ensures that the relevant staff are properly trained in order to enforce the data security conditions.

9. Valoro takes special care of its IT security responsibilities:
    a) measures to protect against unauthorized access, including the protection of software and hardware devices and physical protection (access protection, network protection),
    b) measures to ensure that data files can be restored, including regular backups and the separate, secure management of copies (mirroring, backup),
    c) protection of data files against viruses (virus protection),
    d) the physical protection of data files and the media carrying them, including protection against fire, water damage, lightning and other elemental damage, and the recoverability of damage resulting from such events (archiving, fire protection).

10. Valoro will take the necessary measures to protect paper records, in particular with regard to physical security and fire protection.

11. The employees and other persons acting on behalf of Valoro
    a) the data media they use or possess, including the way in which the data are recorded, shall be securely protected and protected against unauthorized access, alteration, transmission, disclosure, deletion or destruction, and against accidental destruction or damage,
    b) handle personal data in a way that ensures an adequate level of security and confidentiality, including in order to prevent unauthorized access to and use of personal data and the means used to process them.

2. Data protection incident

1. In the event of a data protection incident, the principles of integrity and confidentiality are violated by a breach of the security of personal data which results in the accidental or unlawful deletion, destruction, loss, alteration, unauthorized disclosure, or access to personal data transmitted, stored or otherwise handled. results.

2. 2. Valoro shall take the necessary technical and organizational measures to maintain the security of the processing of personal data and thus to prevent data protection incidents.

3. It is the responsibility of all Valoro employees, natural or legal persons with contractual or other relationships with Valoro, data processors of Valoro, or organizations without legal personality, to prevent the occurrence of data protection incidents.

4. The data protection coordinator shall carry out the detection of vulnerabilities in Valoro's data management activities and security incidents threatening them on a regular basis, but at least when changing technology or using a new data processor. in this context, the data protection coordinator shall assess the risk of data protection incidents, propose measures to mitigate those risks, ensure an adequate level of security of data processing, prevent the occurrence of data protection incidents, taking into account the state of science and technology, and costs related to the nature of the personal data to be protected. the vulnerability assessment shall consider the risks posed by the processing of personal data (such as the accidental or unlawful deletion, destruction, loss, alteration, unauthorized disclosure of, or unauthorized access to, personal data transmitted, stored, or otherwise handled) in connection with the data security risk assessment, which may result in physical, property or non-property damage.

5. The head of any organizational unit or customer's representative may initiate an extraordinary audit of the risk of a data protection incident if there has been a significant change in the data management activities performed or supervised by him or her. the data protection coordinator shall not be obliged to initiate extraordinary checks if it does not consider it appropriate.

6. The Data Protection Coordinator shall initiate an extraordinary review of the risk of a data protection incident in respect of any data management activity that is directly related to another data protection activity affected by a previous data protection incident.

7. If Valoro is required to conduct a data protection impact assessment, the data protection impact assessment should also address the steps involved in dealing with potential data protection incidents.

8. Valoro shall report the data protection incident to the competent supervisory authority through the data protection coordinator without undue delay and, if possible, no later than 72 hours after becoming aware of the data protection incident.

9. The data protection incident shall be reported to the competent supervisory authority and, in the case of data processing, to the customer as soon as possible, taking into account the nature and gravity of the data protection incident, its consequences and adverse effects on the data subject.

10. In the event of a data protection incident involving the supervisory authority and a data processing activity, the notification to the customer shall describe:
    a) the nature of the data protection incident, including, where possible, the categories and approximate number of data subjects and the categories and approximate number of data involved in the incident,
    b) the name and contact details of the data protection coordinator or other contact person for further information,
    c) the likely consequences of the data protection incident,
    d) the measures taken or planned by Valoro to remedy the data protection incident, including, where appropriate, measures to mitigate any adverse consequences of the data protection incident.

11. If the above information cannot be communicated to the supervisory authority at the same time and / or to the client, it may be communicated in detail without further undue delay. The first notification shall indicate that further detailed information will be provided at a later stage. The notification may be executed in installments in particular if the completeness of the notification requires an investigation by the data protection coordinator.

12. If the reporting of a data protection incident is not completed within 72 hours, the report shall also state the reasons for the delay.

13. A data protection incident needs not be reported to the competent supervisory authority if the data protection incident is not likely to pose a risk to the rights and freedoms of natural persons as assessed by the data protection coordinator. In the case of a data processing activity, the customer must still report the data protection incident.

14. 14. Valoro, through the Data Protection Coordinator, shall inform the data subject of the data protection incident as soon as possible without undue delay (with the customer's consent in the case of data processing), if
    a) as a result of the risk assessment of the data protection incident, the data protection coordinator concludes that the data protection incident is likely to pose a high risk to the rights and freedoms of natural persons,
    b) the supervisory authority instructs Valor to inform data subjects of the data protection incident.

15. The information provided to the data subject shall be clearly and intelligibly describe
    a) the nature of the data protection incident,
    b) the name and contact details of the data protection coordinator or other contact person for further information,
    c) the likely consequences of the data protection incident,
    d) the measures taken or planned by Valoro to remedy the data protection incident, including, where appropriate, measures to mitigate any adverse consequences of the data protection incident,
    e) proposals for mitigating possible adverse effects on the data subject.

16. Valoro works closely with the customer, the supervisory authority and follows the instructions given by the customer, the supervisory authority, or another authority (such as the police) to inform data subjects.

17. The data subject need not be informed of a data protection incident if any of the following conditions are met:

a) Valoro has implemented appropriate technical and organizational security measures and these measures have been applied to the data affected by the data protection incident, in particular those measures (such as the use of encryption) that make it incomprehensible to persons not authorized to access personal data the data
b) Valoro has taken further measures following the data protection incident to ensure that the high risk to the data subject's obligation to report the data protection incident is no longer likely to materialize,
c) The information would require a disproportionate effort. In that case, the data subject shall be informed by means of publicly available information or a similar measure shall be taken to ensure that the data subject is equally effectively informed,
d) The supervisory authority determines that one of the conditions set out in points (a) to (c) is met.
e) The customer instructs Valoro to do so.

18. Valoro's internal privacy register includes a record of privacy incidents.

19. The record of data protection incidents contains the following data:

1. Data related to the imminent threat of a data protection incident
   a) date of detection of the imminent threat of the data protection incident (date, hour, minute)
   b) the identity of the observer
   c) the driver informed by the observer
   d) date of threat signal to driver (date, hour, minute)
   e) a description of the threat detected
   f) measures taken by the driver to prevent the occurrence of a data protection incident (date, hour, minute),
   g) date of notification by the data protection coordinator (date, hour, minute)

2. The detection data of data protection incident
   a) time of detection of the data protection incident (date, hour, minute)
   b) the identity of the observer
   c) the date of the notification of the data protection incident to the driver (date, hour, minute)
   d) a description of the data protection incident detected
   e) a description of the measures within its competence to isolate the data protection incident and mitigate any damage, the date of the measure (date, hour, minute)
   f) the date of the notification to the data protection coordinator (date, hour, minute)

3. Data of data protection incident
   a) date of the data protection incident (day, hour, minute)
   b) the nature of the data protection incident
      ba) breach of confidentiality: breach of confidentiality (unauthorized access or disclosure)
      bb) breach of data integrity: breach of the principle of integrity (unwanted alteration of personal data)
      bc) breach of access data: breach of availability (loss of personal data)
   c) description of the data protection incident
   d) the carrier of the data affected by the data protection incident (server, desktop computer, laptop, paper document, etc.)
   e) the number of persons involved in the data protection incident

f) Classification of the person involved in the data protection incident
   fa) natural person customer
   fb) non-natural person customer representative,
   fc) other customer
   fd) Valoro employee, agent, trustee etc.
   fe) other

g) the nature and content of the personal data involved in the data protection incident
   ga) natural identification data (surname and forename, surname and forename at birth, place of birth, date of birth, surname and forename of mother)
   gb) contact details (eg. postal address, electronic address, landline telephone number, mobile telephone number)
   gc) identification or login data (eg. login password, customer number)
   gd) data related to financial information (eg. income, bank card number)
   ge) special personal data
   gf) data related to information society services [eg. the online identifier provided by the device, application, device and protocol used by the person concerned (eg. IP address, cookie ID, radio frequency identification tag)]
   gg) other
   gh) the personal data involved in the data protection incident are not known

h) the reason of the data protection incident
i) the effect of the data protection incident
j) the assessment of the risk of the data protection incident by the data protection coordinator, the level of risk
k) the technical or organizational action taken in relation to the data protection incident
   ka) the content of the measure
   kb) the person responsible for the implementation of the measure
   kc) the deadline for the implementation of the measure

l) A measure to prevent the recurrence of a data protection incident
   la) the content of the measure
   lb) the person responsible for implementing the measure
   lc) the deadline for implementing the measure

4. Date and content of the notification of the data protection incident to the supervisory authority, customer.
5. Action of the supervisory authority related to the customer's data protection incident.
6. Action taken by another authority, customer, related to a data protection incident.
7. Legal proceedings related to the data protection incident.
8. Date and content of informing the data subjects.

9. Data of the third party (eg. data processor) used in connection with the performance of the data processing affected by the data protection incident.

20. The data protection incident procedure should also be provided for Valoro's data processors as described above.

3. Customer audit

Valoro undertakes, in accordance with its data processing agreements, to cooperate in the audit carried out by the customer or its authorized representative, to provide the information and data requested for data protection compliance, without prejudice to the rights and legitimate interests of law, official decision, other customer and data subject.

IX. Chapter
Final terms

1. The present Policy shall apply from 1 January 2022.