Data Protection Guideline

Guideline on processing of personal data within the Nersol Group

1. Introduction

1.1 In order to service our clients the Nersol Group (hereinafter “the Nersol Group” “we” or “us”) needs to collect personal data from our clients and/or potential clients, contact persons at suppliers and/or other business partners. The Nersol Group also processes personal data about employees for the purpose of personnel administration.

In light of the above, the Nersol Group wants to ensure a high level of data protection as privacy is a cornerstone in gaining and maintaining the trust of our clients and/or potential clients, contact persons at suppliers and/or other business partners and thus, ensuring the Nersol Group’s future business. The same applies to the processing of personal data about the employees.

Protection of personal data requires among other things that appropriate technical and organisational measures are implemented to demonstrate a high level of data protection. the Nersol Group has adopted a number of internal and external data protection policies, which must be followed by employees of the Nersol Group.

Additionally, the Nersol Group will monitor, audit and document internal compliance with the data protection policies and applicable statutory data protection requirements, including the General Data Protection Regulation (“GDPR”).

The Nersol Group will also take the necessary steps in order to enhance data protection compliance within the organisation. These steps include the assignment of responsibilities, raising awareness and training within data protection of staff involved in processing operations. Please note that this data protection guideline will be reviewed from time to time to take into account any new obligations. Retention of personal data will be governed by our most recent retention policy.

This data protection guideline, along with guidelines for processing of personal data, constitute the overall framework for processing of personal data within the Nersol Group.

1.2 “*Personal data*” is any information which may be related 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, location data, phone number, age, gender, etc. Such personal data can for instance concern an employee, a job applicant, client/potential client, supplier and other business partners.

1.3 Personal data can be categorized as ordinary non-sensitive personal data or special categories of personal data (sensitive personal data). Special categories of personal data are exhaustively outlined in the GDPR and include personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, bio-metric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation. Ordinary non-sensitive personal data include all information that is not categorized as special categories of personal data (sensitive personal data). Such information can be name, address, telephone number, employee id, information about education, etc. Certain ordinary non-sensitive personal data may be considered confidential. This may, for instance, include information on income and wealth, and information on internal family relationships/matters. Confidential, ordinary non-sensitive data are normally subject to further security measures.

The category of personal data will have an impact on which legal basis the processing of such personal data can be based on. Special rules apply to the processing of data about criminal offences and CPR-numbers. The various legal bases are described below in clause 2.

1.4 Although information regarding companies/businesses is not as such personal data, please note that information relating to contact persons within such companies/businesses, e.g. name, title, work email, work phone number, etc. is considered personal data. However, personal data relating to a personally owned and run business are considered as personal data even if the personal data concern the business. Such personal data are considered as relating to an identified or identifiable natural person.

1.5 The Nersol Group collects and uses personal data for a variety of legitimate business purposes, including establishment and management of customer and supplier relationships, completion of purchase agreements, recruitment and management of all aspects of terms and conditions of employment, communication, fulfillment of legal obligations or requirements, performance of contracts, providing services to clients, etc. When carrying out such processing activities, the first step is to ensure that the general principles relating to the processing of personal data are complied with.

1.6 Pursuant to the general principles personal data shall always be:

- Processed lawfully, fairly and in a transparent manner in relation to the data subject (principle of lawfulness, fairness and transparency);
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (principle of purpose limitation);
- adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (principle of data minimisation);
- 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 (principle of accuracy);
- kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed (principle of storage limitation);
- processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures (principle of integrity and confidentiality).

1.7 The Nersol Group shall be responsible for and be able to demonstrate compliance with the above (principle of accountability). This principle is one of the reasons that we have prepared this data protection guideline and why it is important that you read it thoroughly.

2. Legal basis for the processing of personal data

2.1 Besides complying with the general principles relating to the processing of personal data, the processing of the personal data must also be based on a legal basis. The legal basis will depend on, which category of personal data is being processed.

The most predominant legal bases for processing ordinary non-sensitive personal data, such as, name, address, email, telephone number, credit card information, etc., within the Nersol Group are:

- The performance of a contract to which the data subject is party;

- A legal obligation or requirement to which the Nersol Group is party; and
- Legitimate interests pursued by the Nersol Group or by a third party.

In certain cases, if none of the above legal bases can be applied, the Nersol Group will obtain the data subjects' consent to the processing.

The most predominant legal bases for processing special categories of personal data (if any) within the Nersol Group are:

- Explicit consent from the data subject(s) for one or more specific purposes;
- To comply with obligations and exercising specific rights of the Nersol Group or the data subject in the field of employment and social security and social protection law; and
- If the processing is necessary for the establishment, exercise or defense of legal claims.

Below, follows a more detailed description of the legal bases.

2.2 Performance of a contract

2.2.1 It will be legitimate to collect and process personal data relevant to 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. This applies to all contractual obligations and agreements signed with the Nersol Group, including the pre-contractual phase irrespective of the success of the contract negotiation.

2.3 Compliance with a legal obligation

2.3.1 The Nersol Group must comply with various legal obligations and requirements, which are based on Union or Member State law. Such legal obligations, to which the Nersol Group is subject, may be sufficient as a legitimate basis for the processing of personal data.

2.3.2 Such legal obligations include obligations to collect, register and/or make available certain types of information relating to employees, clients, etc. Such legal requirements will then form the legal basis for us to process the personal data, however, it is important to note whether the provisions allowing or requiring the Nersol Group to process certain personal data also set out requirements in relation to storage, disclosure and deletion.

2.4 Legitimate interests

2.4.1 Personal data will only be processed where it is necessary for the purposes of the legitimate interests pursued by the Nersol Group, and these interests or fundamental rights are not overridden by the interests of the data subject. the Nersol Group will, when deciding to process personal data, ensure that the legitimate interests do not override the rights and freedoms of the individual and that the processing will not cause unwarranted harm. An example of a legitimate interest of the Nersol Group is to process personal data on potential clients in order to expand the business and develop new business relations. The data subject must be given information on the specific legitimate interests pursued by the Nersol Group if a processing is based on this legal basis, cf. clause 4.1 below.

2.5 Consent

2.5.1 If the collection, registration and further processing of personal data on clients, suppliers, other business relations and employees are based on such a person’s consent to the processing of personal data for one or more specific purposes, the Nersol Group shall be able to demonstrate that the data subject has consented to processing of his or her personal data.

2.5.2 A consent shall be freely given, specific, informed and unambiguous indication of the data subject's wishes.
The data subject must actively consent to the processing of personal data by a statement or by a clear affirmative action.

2.5.3 A request for consent shall be presented in a manner, which is clearly distinguishable from other matters, in an intelligible and easily accessible form, using clear and plain language.

2.5.4 To process special categories of personal data (sensitive personal data) the consent shall also be explicit.

2.5.5 The data subject is entitled to withdraw his/her consent at any time and upon such withdrawal, we will stop collecting and/or processing personal data about that person unless we are obligated or entitled to do so based on another legal basis.

2.6 Obligations and exercising specific rights of the Nersol Group or the data subject

2.6.1 This legal basis will in most cases only be relevant if the Nersol Group processes health data about the employees to comply with the rules pursuant to employment law or collective agreements, e.g. reimbursement of sickness benefits, etc.

2.7 Legal claims

2.7.1 This legal basis will be relevant if it is necessary for the Nersol Group to process personal data in order to establish, exercise or defend a legal claim towards a third party, for instance a client or an employee.

3. Processing and transfer of personal data

3.1 The Nersol Group as Data Controller

3.1.1 The Nersol Group is in most cases processing personal data as a data controller, as the Nersol Group determines the purposes and means of the processing of personal data, e.g. when the processing relates to the Nersol Group's clients, other business partners and employees.

3.2 Use of data processors

3.2.1 An external data processor is a company, which processes personal data on behalf of the Nersol Group and in accordance with the Nersol Group’s documented instructions, including for the Nersol Group's purposes and by means set-out by the Nersol Group, e.g. in relation to providers of HR systems, third party IT providers, etc. When the Nersol Group outsources the processing of personal data to data processors, the Nersol Group ensures that said company as a minimum implements the same degree of security measures for the protection of personal data protection as the Nersol Group. If this cannot be guaranteed, the Nersol Group will choose another data processor. The processing by a data processor is governed by a data processing agreement.

3.3 Data processing agreements

3.3.1 Prior to transfer of personal data to the data processor, the Nersol Group shall assess whether the data processor provides sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of the GDPR and ensure the protection of the rights of the data subjects. After the assessment is carried out and it is determined that the data processor meets such requirements, the Nersol Group shall enter into a written data processing agreement with the data processor. The data processing agreement ensures that the Nersol Group controls the processing of personal data, which takes place outside the Nersol Group for which the Nersol Group is the data controller and thereby responsible.

3.3.2 If the data processor/sub-data processor is located outside the EU/EEA, the conditions of clause 3.4.2 below will apply.

3.4 Disclosure of personal data to other independent data controllers

3.4.1 Before disclosing personal data to others, i.e. other independent data controllers, it is the responsibility of the Nersol Group to ensure that the general principles relating to the processing of personal data are complied with. Further, it is the Nersol Group's responsibility to ensure that the disclosure of the personal data is based on a legal basis.

3.4.2 If the third-party recipient is located outside the EU/EEA in a third country that does not ensure an adequate level of personal data protection, the transfer can only be completed if the Nersol Group is providing appropriate safeguards. This will be done by entering into a transfer agreement between the Nersol Group and the third party. The transfer agreement shall be based on the EU Standard Contractual Clauses.

4. Rights of the data subjects

Subject to various terms and conditions and exceptions, the data subjects have the following rights:

4.1 Duty of information when the personal data are obtained from the data subject

4.1.1 When the Nersol Group processes, including collects and registers personal data about data subjects, the Nersol Group is obligated to inform such persons about the following:

- The purposes of the processing for which the personal data are intended as well as the legal basis for the processing;
- the categories of personal data concerned;
- the legitimate interests pursued by the Nersol Group, if the processing is based on a balancing of interests;
- the recipients or categories of recipients of the personal data, if any;
- where applicable, the fact that the Nersol Group intends to transfer personal data to a third country and the legal basis for such transfer;
- the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;
- the existence of the right to request from the Nersol Group access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability;
- where the processing is based on the data subject’s consent, the existence of the right to withdraw consent at any time, however, without affecting the lawfulness of processing based on consent before its withdrawal;
- the right to lodge a complaint with the Nersol Group via the correct procedure or with a supervisory authority;
- whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data;

- the existence of automated decision-making, including profiling, and meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

4.1.2 The Nersol Group has prepared a privacy notice that contains a more detailed description of the above-mentioned information obligation.

4.1.3 If the personal data are not obtained from the data subject, he/she must also be informed about the source from which the personal data originate, an if applicable, whether it came from publicly accessible sources.

4.2 Right to access

4.2.1 Any person whose personal data the Nersol Group is processing, including but not limited to, the Nersol Group employees, job applicants, external suppliers, clients, potential clients, contact persons employed at business partners, etc. has the right to obtain from the Nersol Group confirmation as to whether or not personal data concerning him/her are being processed, and if that is the case, request access to the personal data which the Nersol Group processes about him/her in addition with the information outlined in clause 4.1.1 above.

4.3 Right to rectification

4.3.1 The data subject shall have the right to obtain from the Nersol Group without undue delay the rectification of inaccurate personal data concerning him or her.

4.4 Right to erasure (right to be forgotten)

4.4.1 The data subject shall have the right to obtain from the Nersol Group the erasure of personal data concerning him or her and the Nersol Group shall have the obligation to erase personal data without undue delay, unless it is required by law to retain any information for a prescribed period of time, for example, by financial regulators or tax authorities.

4.5 Right to restriction of processing

4.5.1 The data subject shall have the right to obtain from the Nersol Group restriction of processing, if applicable.

4.6 Right to data portability

4.6.1 The data subject shall have the right to receive the personal data registered in a structured and commonly used and machine-readable format.

4.7 Right to objection

4.7.1 The data subject shall have the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her which is based on a balancing of interests, including profiling.

4.8 Any requests received from a data subject to exercise the rights in this clause will be answered as soon as reasonably possible, and no later than 30 days from receipt. Requests shall be forwarded without delay to the Nersol Group’s Service Center. The Service Center will be supported by the the Nersol Group’s Data Protection Officer to process the request to meet the reply deadline.

5. Data Protection by Design and Data Protection by Default

5.1 New products, services, technical solutions, etc. must be designed so they meet the principles of data protection by design and data protection by default settings why Nersol has implemented the following guiding principles within its organisation:

1. **Privacy as the Default Setting**
Ensure that personal data are automatically protected in any given IT system or business practice.

2. **Privacy Embedded into Design**
Covering business process-, software design and development. Privacy is an essential component of the core functionality and our services, held up without diminishing the functionality.

3. **End-to-End Security — Full Life-cycle Protection**
Ensure that personal data are automatically protected in any given IT system or business practice, using appropriate encryption and authentication until the data is deleted.

4. **Respect for clients Privacy — Keep it Client-Centric**
The users own their data. The consumer has the right to make corrections, including the right to be forgotten.

that inform and support how the Nersol Group fulfils its responsibility to ensure clients' privacy rights.

5.1.1 Data protection by design means that when designing new products or services, key considerations to data protection must be shown.

- The Nersol Group will take the following factors into account when acquiring or developing new products, services, technical solutions, etc.: the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing of personal data.
- The Nersol Group shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, including inter alia as appropriate pseudonymisation, which are designed to implement data protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet data protection requirements and protect the rights and freedoms of data subjects. This is described further in clause 8 below.

5.1.2 Data protection by default requires that relevant data minimisation techniques are implemented.

- The Nersol Group shall implement appropriate technical and organisational measures ensuring that, by default, only personal data which is necessary for each specific purpose of the processing is processed.
- This minimisation requirement applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility.

- Such measures shall ensure that by default, personal data are not made accessible without careful consideration.

6. Records of processing activities

6.1 The Nersol Group shall as data controller maintain records of processing activities under the Nersol Group's responsibility. The records shall contain the following information:

- name and contact details;

- the purposes of the processing;
- a description of the categories of data subjects and of the categories of personal data;
- the recipients to whom the personal data have been or will be disclosed, including recipients in third countries or international organisations;
- where applicable, transfers of personal data to a third country, including the identification of that third country and, if relevant, the documentation of suitable safeguards;
- where possible, the envisaged time limits for erasure of the different categories of data; and
- where possible, a general description of the applied technical and organisational security measures.

6.1.1 The Nersol Group shall make the records of processing activities available to relevant data protection authorities upon request. the Nersol Group has prepared several of such records.

7. Deletion of personal data

7.1 Personal data shall be deleted when the Nersol Group no longer has a legitimate purpose for the continuous storage or other processing of the personal data, or when it is no longer required to store the personal data in accordance with applicable legal requirements.

7.2 Detailed retention periods with respect to various categories of personal data are specified in the Nersol Group's Data Retention and Information Sharing policy.

8. Security of processing (risk assessments)

8.1 The Nersol Group shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:

- The pseudonymisation and encryption of personal data;
- the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
- the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
- a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

8.2 In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed. the Nersol Group has prepared written risk assessments with regards to the processing activities.

9. Data Protection Impact Assessment

9.1 If the Nersol Group processes personal data that is likely to result in a high risk for the persons whose personal data is being processed, a Data Protection Impact Assessment ("DPIA") shall be carried out.

9.1.1 A DPIA implies that the Nersol Group will, taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and

freedoms of natural persons, implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with data protection requirements.

9.2 The technical and organisational measures shall be reviewed and updated where necessary and no later than every 6 months.

9.2.1 Adherence to approved codes of conduct or approved certification mechanisms may be used as an element by which to demonstrate compliance with the appropriate technical and organisational measures according to this clause.

10. Profiling

10.1 Pursuant to the GDPR, profiling is defined as "*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 analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements*".

10.2 “Profiling” in the context of this data protection guideline is the use of an automated process to analyse personal data in order to assess or predict aspects of a person’s behaviour. the Nersol Group may use profiling in the following circumstances:

- To help identify potential cases of financial crime;
- To provide clients and leads with information on the Nersol Group products and services that seem likely to be of their interest; and
- To asses creditworthiness

11. National requirements

11.1 The Nersol Group shall comply with GDPR for its internal process and procedures.

11.2 If national legislation requires a higher level of protection for personal data than the GDPR, such stricter requirements are to be complied with. If the Nersol Group’s policies/guidelines are stricter than the local legislation, our policies/guidelines must be complied with if applicable to the services provided or processing being done.