GDPR Policy Metrostav Norge AS

1. Introduction

Metrostav Norge AS is committed to protecting the right to privacy of its employees and everyone with whom it does business. The purpose of this document is to set out the principles according to which personal data will be handled in accordance with applicable data protection laws. This includes the EU Data Protection Regulation 2016/679 ("GDPR").

The Data Protection Advisor at Metrostav Norge AS is responsible for implementing and monitoring the procedure.

2. Data Protection Policy

2.1. General

We will process personal data in accordance with the following principles set out in applicable privacy and data protection legislation.

2.2. Main principles

Principle 1: Legality, fairness and transparent information

Fair treatment: we will refrain from processing personal data in a way that is unreasonably harmful, unexpected or misleading to the individuals concerned.

Transparent handling: we will be clear, open and honest with the subjects of data processing and storage inform you of the purposes for which and how we process their personal data.

Legality: we will ensure that all processing of personal data has a legal basis.

Principle 2: Limitation of purpose

We will only process personal data for specific, explicit and legitimate purposes.

Specific and explicit: we will specify the purpose for each processing activity.

Legitimate: the purpose must be justified in relation to our business.

We will not process personal data for purposes that are incompatible with the original purpose which the personal data was collected.

We can process anonymous data without restriction because it is no longer personal data.

Principle 3: Data minimization

We will only process personal data which is relevant and necessary for the original purpose, and we will:

• Identify the types of personal data processed so we can assess the necessity of the data.

• We instruct employees to avoid the use of identifiers (where practicable) and to limit the amount of personal information in documents and forms, whether electronic or printed.

Principle 4: Data accuracy

We will take appropriate measures to ensure that personal information is accurate, complete and, where necessary, up to date. To achieve this:

• we will put in place appropriate procedures for the collection of personal data to ensure the accuracy of the data entered.

• we will put in place appropriate procedures for regular or ad-hoc checks of systems and documents containing personal data requiring maintenance to ensure that the data is up to date.

• we will put in place appropriate procedures to allow data subjects to request access to their personal data and to request the rectification, completion and updating the personal data.

Principle 5: Storage limitation

We will not retain personal data for longer than is necessary for the purpose for which it was collected. To do this:

• we will specify the expected storage period (i.e. when the personal data must be deleted), including the reason for the storage period.

• we implement automatic deletion procedures to a reasonable extend.

• if the deletion routines will be manual, implement scheduling, alert systems or other mechanisms to ensure compliance with the routines.

• we support the use of archiving and communication systems/platforms to reduce unstructured data.

• where the personal data is kept for latent purposes (e.g. to defend potential claims), but are not otherwise necessary for day-to-day operations, appropriate measures will be taken to restrict access to the data and prevent the use of the data in day-to-day operations (blocking or restricting access). This archived data will be pseudonymized (de-identified, e.g. by replacing the name/ID identifier).

• we will consider anonymization as an alternative to deletion if the data can continue to serve a purpose in anonymized form. Anonymization means that the data is unlikely to be re-identifiable by usual means.

• if system constraints require backup data to be retained after the retention period has expired, ensure that the backup data is subject to strict access control and is not used operationally.

Principle 6: Integrity and Confidentiality

We will ensure adequate security of personal data as further described below.

3. Legal basis

3.1. General

We identify the applicable legal basis for each processing activity. If no legal basis can be identified as valid, such activity will be terminated.

For the processing of personal data that are not special categories of personal data (sensitive personal data), we may rely on one of the following legal bases under Article 6 of the GDPR:

Legal basis	Description	Requirements	Examples of use
Agreement	The processing of the data is necessary for the performance of a contract with the data subject or for taking steps before entering such a contract.	The contract must be concluded with the data subject. At this legal basis cannot be relied upon in the case of an agreement with commercial partners (legal persons).	Recruitment HR administration Payroll
Legitimate interests	The processing of data is necessary for the achievement of a legitimate interest, insofar as it is over and above this interest does not override the rights and interests of data subjects.	A legitimate interest is identified by us or a third party (e.g. a commercial partner); the data are necessary to achieve the interest; and, after considering the interest of the legitimate interest outweighs the rights and interests of the data subject.	Contract management with commercial Partners Mergers & Acquisitions HR Administration Payroll
Legal obligations	The processing of data is necessary for compliance with a legal obligation set out in the laws of EU/EEA Member States.	The legal obligation must be expressly or implicitly provided for in the law of an EU/EEA Member State.	Accounting Security
Vital interests	Data processing is necessary to protect vital the interests of the data subject	The question of life and death	Emergency response

Public interest	The processing of data is necessary for the performance of the tasks carried out by a public authority or private organizations acting in the public interest.	Exercise of official authority.	Public information
Legal basis	Description	Requirements	Examples of use
Consent	The data subject has consented to the processing.	Consent must be given in accordance with GDPR Article 7.	Use of employee images on the intranet or the internet Storage of data on unsuccessful applicants after the recruitment process

3.2. Sensitive data

In addition, for special categories of data (sensitive data) we must have a legal basis under Article 9 of the GDPR. Sensitive data are data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership and the processing of genetic data, biometric 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.

When processing this sensitive personal data, we identify one of the following legal bases:

Legal basis	Description	Requirements	Example of use
Employment	The processing of data is necessary for the purposes of fulfilling obligations and exercising specific rights in the field of labor law and social security and social protection law.	It must be authorized by law in each EU/EEA member state.	Sick leave management. Adjusting the workplace for health reasons. Alcohol or drug tests in the workplace, if required by for security reasons.
Life interests	Data processing is necessary to protect vital the interests of the data subject if the data subject is unable to give consent.	The question of life and death	Emergency response

Public data	The data processing relates to personal data that the data subject apparently discloses	The data subject clearly had to disclose the data.	Public relations (e.g., handling a person's published party affiliation).
Legal basis	Description	Requirements	Example of use
Legal obligations	The processing is necessary for the establishment, exercise or defense of legal claims.	The claim may be supported by law, contract or otherwise.	Responding to binding summonses from public authorities.
Consent	The data subject shall by processing explicitly he agreed.	Consent must be given in accordance with GDPR Article 7.	Access control from contractors.

3.3. Criminal prosecution and conviction

We may only process personal data relating to criminal offences and convictions if they have a legal basis, either consent, vital interest or legal claims as described above.

Criminal convictions data are data relating to persons sentenced to, fines or other criminal penalties by the courts (or similar competent authorities), as well as questions and answers relating to whether an individual has a criminal record.
Criminal data is data relating to criminal charges or proceedings.

3.4. Unique identifiers

We may only process birth numbers and other unique identifiers where there is a legitimate need for specific identification and the method is necessary to achieve such identification. We will not process social security numbers and other unique identifiers for verification purposes.

4. Transparency

4.1. General

We will be transparent about all data processing activities and provide data subjects with all information about data protection.

4.2. Content of the data protection information

We will inform data subjects of why and how their data is processed, in accordance with Articles 13 and 14 of the GDPR. The information must be clear and unambiguous. The privacy information will be regularly reviewed to ensure that it is up to date.

4.3. Communication of information on data protection

We will make sure that information about data protection is easily accessible, for example in contracts and on our website. We will also provide relevant data protection information upon the data subject's

request.

4.4. Rights of the data subject

We will respect the rights of data subjects to data processing, including the right of access, rectification, erasure, restriction and the right to object.

4.5. Automated decision making

We may use automated decision-making, including profiling, that has legal effects on or similarly affects data subjects. An example is automated assessment of job applications in recruitment. We will comply with the requirements of Article 22 of the GDPR for such decisions.

4.6. Marketing

We may conduct limited marketing activities. We may send direct marketing via email to the following recipients: those who have consented or those who are existing business partners. Recipients will have the option to opt-out of future email marketing.

4.7. Privacy by design and privacy by default

Where we develop (in-house or through service providers) software, platforms or other solutions, we will put in place appropriate measures designed to implement data protection policies as an integrated feature. We will configure such solutions to limit the amount of personal data, the scope of data processing and the retention period to a minimum by default.

4.8. Joint control

Joint control exists when two or more controllers jointly determine the purposes and means of processing, either within the group or regarding external business partners.

Where we (as controllers) cooperate with one or more other controllers (or external entity) in relation to the processing of personal data, it will be assessed on a case-by-case basis whether they are acting as joint controllers. As a starting point for such an assessment, we will consider joint control to be likely if the parties pursue the same overall objectives and mutually contribute to the processing of data.

If we that there is joint control, joint administrator agreement will be concluded. Such an agreement will identify the respective responsibilities of the parties for compliance with applicable laws and regulations, including the obligation to provide privacy information to data subjects and the roles and responsibilities to data subjects with respect to handling data subject rights requests.

5. Transfer to non-EU/EEA countries

All countries within the EU/EEA region have implemented the GDPR to ensure proper handling of personal data.

To be able to transfer or process personal data outside the EU/EEA, it must be ensured that the appropriate level of protection. This can be ensured by complying with the standard protection rules adopted by the European Commission (Standard Contractual Clauses).

6. Data processors with personal data

We use the following four-step approach to engage processors:

Step 1: Determine roles

First, we determine whether the entity is acting as a processor. A processor is a company that processes personal data for us without independently determining why the processing is taking place, what data is to be processed and how long the data is to be kept.

Step 2: Screening

Before engaging a processor, we will verify that the processor provides sufficient safeguards to meet the requirements of applicable data protection laws. We may do this by requesting relevant documentation and information on data protection in the procurement process or by other appropriate means.

Step 3: Conclusion of the data processing contract

We will enter into a data management agreement with each processor. Such the contract may be in addition to another contract (such as a service contract).

Step 4: Audit

We will verify compliance with the data processing agreement.

We may ask the processor to prepare regular data security reports. We will review the report and assess the adequacy of the data security and privacy measures. If the report reveals warning signs, we will ask for further information. If we have reason to believe that the processor's data security or privacy standards are inadequate, we will conduct a more thorough audit. If we are not satisfied with the level of data security or privacy standards, we will terminate the contract.

7. Sharing data with independent administrators

Whenever we as a controller share personal data with another separate controller, we will consider formalizing this agreement on the protection of personal data against unlawful processing.

Whenever we, as a controller, receive personal data from another independent controller, we will consider imposing a contractual obligation on such controller to notify data subjects that we are the recipient of personal data to support such controller in complying with GDPR Article 13.

8. Records of processing activities

We will establish records of processing activities. The purpose of these records is to ensure compliance with Article 30 of the GDPR and to facilitate compliance with other GDPR requirements. The Norwegian supervisory authority Arbeidstilsynet's template will be used to create the records of processing activities.

It is the responsibility of each data processor to complete and maintain such records. The data processing owner is a role that has functional responsibility.

9. Data security

We will put in place and maintain appropriate technical and organizational measures to ensure an adequate level of data security to prevent accidental or unlawful destruction, loss, alteration, unauthorized disclosure of or access to personal data transmitted, stored or otherwise processed.

For personal data, we will ensure that data security measures take due account of the following aspects:

Safety criteria	Definition	Description / Examples
Confidentiality	Protection against unauthorized access or disclosure of data.	1. Employees and business partners will be subject to a reasonable duty of confidentiality. 2. The databases will be encrypted and subject to appropriate access controls. 3. Agreements with IT vendors will include commitments on data security. 4. Physical facilities will be adequately protected against unauthorized access.
Integrity	Protection against unauthorized modification or deletion of Data.	1. The databases will be encrypted and subject to appropriate access controls. 2. Key documents will have version control (revision history).
Accessibility	Access to data in case of need.	1. Agreements with key IT service providers will have appropriate terms and conditions. 2. The material data will be remotely accessible (VPN or similar).
Resilience	Business continuity is ensured.	1. Agreements with key IT service providers will have appropriate commercial terms. 2. The data will be backed up.

10. Addressing data leaks

We may potentially experience a personal data breach - a breach of security resulting in the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data. If this occurs, we will assess within 72 hours whether we need to notify data subjects and/or the relevant data protection authority.

Employees who suspect or become aware of untoward incidents related to the processing of personal data shall immediately report the incident to their line manager, HR manager or the Data Protection Advisor. The Data Protection Adviser shall be responsible for informing the competent Data Protection Authority.

11. Privacy risk assessment

We will conduct general privacy risk assessments of our business on a regular basis. The purpose of such assessments is to identify potential privacy risks and to identify measures appropriate minimize those risks. In the context of privacy, the risks (adverse consequences of an event) are in particular: Physical harm; Discrimination; Identity theft; Fraud; Financial loss; Damage to reputation; economic or social disadvantage; unauthorized disclosure of or access to special categories of data; Unauthorized disclosure of or access to data relating to personal aspects such as economic situation or job performance evaluation.

The risk assessment should consider at least: (i) the level of acceptable risk, (ii) the potential adverse events, (iii) the likelihood of those events occurring, (iv) the privacy implications if the event occurs, and (iv) if the risk is unacceptable, measures to address the risk.

12. **Data Protection Impact Assessment**

If a processing operation, such as the use of a new technology, is likely to result in a high privacy risk, considering its nature, scope, context and purpose, we will carry out a Data Protection Impact Assessment (DPIA).

The DPIA must contain at least (i) a systematic description of the intended processing operation, (ii) an assessment of its necessity and proportionality, (iii) a privacy risk assessment and (iv) measures to address the risks.

13. Identification of the principal supervisory authority

Where communication with a supervisory authority is required in relation to cross-border processing involving more than one EEA country, a lead supervisory authority must be identified.

The supervisory authority is the authority of the country in which our main establishment is located. The main establishment shall be located at the place of our central administration, unless decisions concerning the purposes and means of processing are taken at another establishment which has the power to make such decisions.

14. Training

We will provide data protection and privacy training to our employees.

Personnel with permanent or regular access to personal data who are involved in collecting personal data or developing tools used to process personal data, receive mandatory training on privacy and data protection. Relevant staff should be defined according to their exposure to the processing of personal data in the context of their position and daily tasks. Relevant personnel are:

• HR department that manages HR data.

• Safety functions, specifically health and work environment personnel, safety incident response personnel to include identified individuals and emergency response personnel teams

• Corporate audit

• IT functions, more specifically information security, application support and other intergroup IT services

• Line managers