POLICY ON PRIVACY AND DATA PROTECTION

EUROPRIS ASA

(Adopted by the board on 28 January 2025)

1. Introduction

The term ”data protection” in this policy refers to legislation and regulations imposed on businesses to ensure that personal data (data related to a physical person) are collected, made available or otherwise treated in a correct and legal manner. This includes general privacy rules under the Personal Data Act, as well as specific provisions such as Section 104 of the Copyright Act concerning depicted individuals, and the Working Environment Act regarding access to employees' emails. The group maintains an up-to-date documentation system called Internal Control GDPR, which includes internal risk assessments and other documentation related to data protection and privacy. The group must externally, through privacy statements and contractual agreements, demonstrate that data protection and privacy are handled in accordance with these minimum requirements.

The privacy legislation prohibits the processing of special categories of personal data, unless an exception in the General Data Protection Regulation (GDPR) article 9(2) is fulfilled. For general personal data, there are a number of legal conditions concerning collection, storage and processing in the general rules of the Personal Data Act and GDPR.

The purpose of this policy is to provide group employees with a basic understanding of circumstances which are typically regulated by data protection legislation, and thereby facilitate compliance with such legal requirements in the group.

This policy applies to *everyone* in the group – all employees, contractors, managers, senior executives and directors (who are all included in the term “employees” when used in this policy).

In addition to these general guidelines, special requirements set in local data protection legislation must be complied with by all employees responsible for and involved in processing personal data. The group's internal GDPR compliance system, with checklists and other documents, is followed to ensure the group meets current data security requirements. The group shall conduct self-assessments of its routines and policies regarding personal data and information security to ensure they are appropriate, adequate, and up-to-date in relation to internal and external factors. This includes performing an annual GDPR self-assessment and a risk assessment prior to any new processing of personal data (e.g., use of a new data processor, new cloud service, or new app).

2. Summary

- The privacy legislation restricts the categories of personal data which can be collected, regulates the circumstances of such acquisition, and determines how long such information can be stored.
- Proposals for acquiring data (such as collecting personal information on employees or customers or purchasing customer information through websites) must be carefully analysed to ensure that they do not breach privacy legislation.

- The need for proportionality and access are key concerns, and all individuals registered must be informed of the group's acquisition and processing of their personal data, for instance, by presenting a privacy notice tailored to the processing activities.
- Personal data must only be shared with third parties when a legitimate purpose exists and only when adequate measures have been taken, such as an agreement on data protection with the third party (a data processing agreement if the third party processes personal data on behalf of the group).
- Transferring personal data to entities outside the European Economic Area (EEA) or accessing such information outside the EEA must only occur if the exporting entity has received assurances from the importing entity that the personal data are adequately protected.
- Data security breaches could result in compensation claims, fines or imprisonment, in addition to administrative sanctions from regulators.

3. Processing of personal data

"Personal data" is any and all information which relates directly or indirectly to an identified or identifiable physical person. Such data must only be collected for specified, explicit and legitimate purposes and not utilised more than is necessary and compatible with the purpose. If a legitimate purpose cannot be established in accordance with national legislation, the data must not be collected.

"Processing of personal data" means any and all operation or set of operations conducted with the information, regardless of whether this is done using automated tools. These include but are not limited to acquisition, organisation, storage, customisation, sharing, blocking, adaptation or modification, use or deletion.

Processing personal data is only legitimate if the processing has a lawful basis, which for the group may be one of the following:

- the individual to whom the personal data applies has consented to the purpose of the processing
- the processing is necessary to fulfil a contract to which the individual is party, or to act on the individual's enquiries before entering into a contract
- the processing is necessary for compliance with a legal obligation of the group
- the processing is necessary for executing a duty in the public interest or in the exercise of official authority given to the group or
- the processing is necessary for the legitimate purposes of the group or of a third party with whom the personal data are shared, except in those cases where the interests of the individual to whom the personal data applies are regarded as more important than the group's interest in processing the data for the stated purpose.

For the group, most processing activities are necessary due to contractual agreements or legal obligations. Pursuant to applicable legislation or, in other cases, as far as is practical and reasonable in the circumstances, personal data must be collected only with the consent of the individual concerned. The consent of individuals whose personal data are being collected must be

unambiguous, explicit and revocable at the individual's request. If neither contract, legal obligation nor consent is applicable, the group should assess whether it has a legitimate interest (a legitimate goal where the balance of arguments are in the group's favour), otherwise such processing of personal information should not be carried out.

When acquiring personal data, the proportionality of the acquisition and the opportunities for control and access must be assessed. The personal data collected must be adequate, relevant and not superfluous to the purpose which the information is being collected and/or processed for. Personal data must be processed in accordance with the applicable data protection declaration on the group's website or made readily accessible to individuals affected by the processing (e.g., the employee handbook or intranet can be used to inform employees).

4. Sensitive personal data and specified categories of personal data

"Sensitive personal data" refers to special categories of personal data as well as personal data about criminal convictions and offences. Sensitive personal data should not be collected unless such collection is considered absolutely essential and is legal under current legislation.

Special categories of personal data include personal information about racial or ethnic origin, political views, religion, philosophical beliefs, or trade union membership, health information, data on sexual relationships or orientation, and genetic and biometric information aimed at uniquely identifying a physical person.

Other categories of personal data which are sensitive but nevertheless require special protection pursuant to applicable legislation must be processed in accordance with the need for protection.

Examples of specific categories of personal data include but are not limited to:

- information related to breaches of the law, criminal convictions or security measures supervised by a government authority
- credit information
- medical data
- children's personal data
- personal identification number (an 11-digit personal identification number can only be processed when there is a factual need for secure identification, and it is needed to obtain that identification)

5. Information on acquiring personal data

When required by applicable legislation or, in other cases, as far as practical and reasonable in the circumstances, individuals must be informed about the processing of their personal data. Such information must, as a minimum, contain the following details:

- name of the legal entity which determines, alone or together with others, the purpose for which the personal data is processed (designated as the data controller)
- the purpose of processing the personal data
- all the information required for the individual to be able to protect their rights in connection with the processing, such as the various types of personal data involved, the recipients of the various categories of personal data, and what access the individual has to this information pursuant to applicable legislation as specified in point 6.

6. Requests for access to information

If an individual wishes to receive information about the group's processing of personal data, or wants to correct errors in their personal data, the group will respond in accordance with the requirements in applicable legislation and otherwise in accordance with the requirements which can reasonably be specified in consultation with the person responsible for privacy and date protection in the group.

7. Quality, confidentiality and security

Accuracy: Processed personal data must be accurate and updated to the extent necessary. Personal data which are inaccurate or incomplete will be deleted or corrected.

Limitation of purpose: Personal data must only be collected for specific, explicitly stated, and legitimate purposes and must not be further processed in a manner incompatible with those purposes.

Data Minimisation: Personal data must be adequate, relevant, and limited to what is necessary for the purposes for which they are processed.

An employee with access to personal data must only process them in accordance with the purpose of the processing and must not utilise the personal data, share it or in other ways distribute it to a third party unless instructed to by the group.

Integrity and Confidentiality: Personal data must be processed in a manner that ensures adequate security, including protection against unauthorised or unlawful processing and against accidental loss, destruction, or damage, by using appropriate technical or organisational measures.

Suitable technical and organisational measures must be implemented to protect personal data against illegal or erroneous destruction, erroneous loss or change, unauthorised sharing or access, or any and all forms of illegal processing. The scope of such measures must be tailored to risks posed by processing personal data and the nature of the information.

Breaches of the safety measures which weaken the confidentiality or security of personal data processed by the group must be reported immediately to a superior and to the person responsible for data protection in the group.

8. Storage

Storage limitation: Personal data must be stored in such a way that it is not possible to identify the individuals for longer than necessary for the purposes for which the personal data is being processed.

Personal data must only be stored for as long as is necessary with regard to the purpose to be fulfilled by acquiring the information, and in accordance to applicable legislation on storage of personal data.

When the storage period has expired, the information must be deleted in a safe and permanent way.

9. Sharing

Personal data must only be shared with third parties, such as the group's sub-suppliers, partners and collaborators, providing a legitimate purpose exists. When personal data are shared with a third party, a written decision must be produced to specify whether the third party is the data controller or data processor of the personal data concerned. This may be documented, for example, by specifying the role in a completed Data Processor Checklist for the relevant processor, or through the Record of Processing Activities for Europris, where the data controller indicates this.

The term ”data processor” refers to a legal entity which processes personal data on behalf of a data controller. The term ”data controller” refers to a legal entity which singly or together with others determines the purpose of and funding for the processing of personal data.

Where required pursuant to applicable legislation, an agreement on data processing (data processor agreement) must be entered into with each data processor – in connection, for example, with using cloud service or outsourcing IT services.

Such agreements must require that the data processor protects personal data from further sharing and only processes the information as instructed by the group. A data processing agreement must also require that the data processor implements sufficient security measures to protect the personal data and undertakes to keep the information confidential, as well as including procedures for reporting breaches of these measures.

10. Transfer of personal data

Transferring personal data to entities outside the European Economic Area (EEA), or accessing the personal data of entities outside the EEA, is only permissible when the exporting entity has received assurances that the personal data are adequately protected by the importing entity.

The group’s standard agreements for transferring personal data to a third party in unsecured third countries must be based on templates called Standard Contractual Clauses, approved by the European Commission in 2021, and these need to be completed by entering detailed information on the third party.

11. Marketing measures and websites

Using personal data for marketing measures, such as direct marketing campaigns, marketing through social media, or the purchase of personal data for marketing purposes, must comply with applicable legislation. Unless legitimate grounds make it necessary to acquire and use such information for marketing measures, personal data must not be utilised for such functions.

Individuals have the right to oppose the processing of their personal data for marketing purposes. If an individual expresses such opposition, the group is duty bound to comply with their wish.

All the group’s external websites must carry a privacy statement including procedures (for example, use of cookie tools) for accepting cookies which accord with the requirements posed by applicable legislation.

12. Reporting activities related to processing personal data

The group shall update its internal control system for GDPR compliance at least annually, and relevant parts of such documentation shall be made available to the Norwegian Data Protection Authority (Datatilsynet) upon request.

In the case of major breaches of personal data security (such as hacking attacks or loss of personal data), the group is obligated to promptly notify the Data Protection Authority. Notification must occur without undue delay and no later than 72 hours after the breach or suspected breach was discovered.

13. Sanctions

Sanctions for breaching data protection legislation include compensation claims from individuals whose personal data have been unlawfully processed, as well as fines and imprisonment. In addition,

the regulator can prohibit the group from conducting various forms of processing and impose administrative sanctions.

14. Dos and don'ts

DO:

- Take particular care when acquiring and processing sensitive personal data and other special categories of such information.
- Give necessary information to individuals and respond to requests for access to the extent that this is required by applicable legislation – and in other cases as far as practical and reasonable in the circumstances – in consultation with the person responsible for privacy and data protection in the group.
- Keep personal data confidential and implement the necessary security measures tailored to the risks posed by processing the personal data, and on the basis of the nature of this information.

DON'T:

- Acquire personal data without an established goal for their processing and without specifying a period of time when this goal is relevant.
- Acquire personal data on the basis that they are "good to have".
- Share or transfer personal data, even to the group's partners, without taking adequate steps – such as a data processing agreement.

15. Reporting

Employees who suspect breaches in the group of the guidelines in this policy, or of relevant data processing legislation, must contact the CFO or the data protection official in the group.

16. Training

The group must conduct adequate training and education of all employees in accordance with the group's risk profile and on the basis of the individual employee's area of responsibility.

***