POLICY ON DATA PROTECTION

EUROPRIS ASA

(Adopted by the board on 1 February 2023)

1. Introduction

The term ”data protection” in this policy refers to legislation and regulations imposed by states to ensure that personal data (or information related to a physical person) are collected, made available and otherwise treated in a correct and legal manner.

Data protection legislation prohibits processing a number of categories of personal data, other than in exceptional circumstances. The remaining categories of personal data, which can be legally processed, are also subject to a number of legal conditions concerning acquisition, storage and processing.

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, 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.

2. Summary

- Data protection legislation restricts the categories of personal data which can be acquired, 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 data protection 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.
- 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.
- 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.
- Breaches could result in compensation claims, fines or imprisonment in addition to administrative sanctions from regulators.

3. Acquiring personal data

"Personal data" is any and all information which relates directly or indirectly to an identified or identifiable person. Such data must only be acquired 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 acquired.

"Processing personal data" means any and all operations or combination 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 or deleting. Processing personal data is only legitimate if:

- the individual to whom the personal data applies has consented
- the processing is necessary for executing a contract which the individual is party to, or to act on the individual's enquiries before entering into a contract
- the processing is necessary for compliance with legally regulated duties which are binding on the group
- the processing is necessary for executing a duty to comply with official purposes or in the exercise of official authority given to the group or to a third party the data are shared
- the processing is necessary for the legitimate purposes of the group or of a third party with whom the data are shared, except in those case where the private interests of the individual to whom the personal data applies are regarded as more important.

Pursuant to applicable legislation or, in other cases, as far as is practical and reasonable in the circumstances, personal data must be acquired only with the consent of the individual concerned. The consent of individuals whose personal data are being acquired must be unambiguous, explicit and revocable at the individual's request.

When acquiring personal data, the proportionality of the acquisition and the opportunities for control and access must be assessed. The personal data acquired must be adequate, relevant and not superfluous to the purpose which the information is being acquired and/or processed for. Personal data must be processed in accordance with the applicable data protection declaration published at any given time on the group's website.

4. Sensitive personal data and specified categories of personal data

"Sensitive personal data" are information about the person concerning their ethnic origin, political views, religious or philosophic views, organisational affiliation, health or sexual orientation. Sensitive personal data must not be acquired unless this is considered absolutely essential, and is legal pursuant to applicable legislation.

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.

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 (in some cases designated 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 data protection in the group.

7. Quality, confidentiality and security

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

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.

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

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.

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 must be entered into with each data processor – in connection, for example, with using the cloud 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 are based on templates approved by the European Commission. 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 accepting cookies which accord with the requirements posed by applicable legislation.

12. Reporting activities related to processing personal data

The group is required to report on its activities related to processing personal data to an official regulator, unless it can rely on an exemption from this duty.

Should changes occur to the group's activities related to processing personal data, an assessment must be made of whether reporting to the regulator needs to be updated or amended.

13. Sanctions

Sanctions for breaching data protection legislation includes 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 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.

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.

***