

FORCIT GROUP DATA PROTECTION POLICY

INTRODUCTION AND PURPOSE

FORCIT Group stores and processes personal data relating to former, current and potential employees of the whole FORCIT Group and the former and current employees of external business partners (e.g. customers and suppliers) and other external stakeholders.

Personal data refers to information or data associated with an identified or identifiable natural person. This includes among other things name, address, social security number, physical address, IP address, photographs, health related data and other types of data that on its own or combined with other data discloses something about the person in question.

The purpose of this Data Protection Policy is to ensure that FORCIT Group complies with the GDPR, national data protection legislation and other legislation that concerns the processing of personal data. The relevant national laws will take precedence in the event they conflict with this Policy.

FORCIT Group complies with the EU's General Data Protection Regulation (2016/679) and the provisions of other related laws and standards. This Policy applies to all companies and operating countries of the FORCIT Group.

SCOPE

This policy applies to all personal data being processed by any employee of FORCIT Group in relation to FORCIT Group operations regardless of the location or device where that personal data is stored and/or processed (e.g., on a FORCIT Group owned or on an employee's own device) and regardless purpose of the data and the reason the data is accessed.

PRINCIPLES

FORCIT Group will collect, process and store personal data according to the following principles.

- Lawful, fair and transparent
- Only for specified, explicit and legitimate purposes.
- Adequate, relevant and limited to what is necessary for the purposes of the data
- Accurate and, where necessary, kept up to date
- With adequate and up-to-date security tools and processes to protect against unauthorized access to the data.

OUTSOURCING THE PROCESSING OF PERSONAL DATA

FORCIT Group (data controller) may outsource some processing activities to one or more external data processor. These external data processors must always have sufficient technical

and organisational resources and processes to ensure that all personal data is processed securely and in compliance with data protection laws.

REPORTING PERSONAL DATA BREACHES

Every employee of the FORCIT Group is obligated to report all personal data breaches (actual or suspected) to the FORCIT Group ICT and HR organizations immediately. Persons (internal or external) suspect that the processing of their personal data may violate this FORCIT Group Data Protection Policy should contact FORCIT Group ICT and HR organizations as soon as possible.

Forcit Group will report all the actual personal data breaches to the appropriate authorities according to the local laws and regulations. FORCIT Group will also contact all the persons whose personal data has been or may have been breached without undue delay.

Joakim Westerlund, CEO

Stefan Långström, Chief People and Culture Officer

Jami Kangasoja, ICT Manager