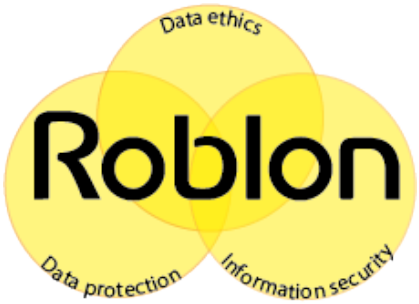
As it is central to the operation of Roblon's business that our business partners have confidence in us and how we process their data, we are dedicated to protecting data in three ways:



1) Information security
   Roblon is highly focused on maintaining a high level of information security by assessing risks and mitigating them by implementing security measures. A separate IT security policy has been established.

2) Data protection
   Roblon is very focused on complying with data protection rules and protecting user rights at all times in our processing of data.

3) Data ethics
   Furthermore, we have laid down Roblon's data ethics rules in this data ethics policy to ensure that we are able, from an individual as well as a societal perspective, to preserve the our business partners' confidence in how we process data.

This data ethics policy cannot stand alone and should be considered a supplement to local statutes and guidelines as well as Roblon's existing data protection and IT security policies.

Data ethics principles

Roblon is very focused on ensuring that data are processed in an ethically responsible manner. As data may comprise more than personal data, this supplementary data ethics policy is required.

1) Dedication to data ethics

   Roblon has appointed a team to drive and maintain the Company's focus on data ethics. The team is responsible for assessing data ethics issues and escalating them to Management. Roblon's Management is dedicated to ensuring that the data ethics principles are embedded in the day-to-day operations. Management also ensures that the Company has an approved data ethics policy.

2) Data processing responsibility

   Roblon takes responsibility for the processing of data, both in the existing set-up and in relation to future systems. This applies to internal data as well as to data we process in connection with customers and suppliers. We only store relevant data for clearly defined purposes and ensure that we are in compliance with applicable legislation, rules and conventions.
   The purpose is to minimise the risk of unintended consequences of the use of data.

3) Guidelines on third-party data processing

   We ensure that IT suppliers act under instruction, maintain a high security level in their data processing and are dedicated to ensuring that data are handled in an ethical manner. Accordingly, third parties must comply with our IT security and data protection requirements and must know how to operate on the basis of data ethics.
   Roblon does not sell data and does not disclose data unless required to do so.
   When new technologies are commissioned, they should be assessed on the basis of these data ethics principles.

4) Value and security for customers

   Data are used to create value for our customers by making their access to the right solutions and offers as efficient as possible.
   We strive to give our customers and suppliers assurance that their data will be processed responsibly and securely.
   We assess on an ongoing basis whether data can have adverse consequences when new processing of data is initiated, including when new technology is commissioned.

5) Employees are trained and data processing controlled

   All relevant employees receive instruction in the secure, lawful and ethical processing of data.
   Instruction is provided by means of external courses and internal information campaigns.
   We perform regular controls of security, processing of personal data and data ethics.

Audit

This policy is reviewed and approved annually by Roblon's Executive Management. The policy forms the basis of our data ethics reporting in the management's review.

Controls

As a supplement to existing controls and audit relating to information security and data protection, the following controls are performed annually to ensure compliance with the data ethics policy:

1.1 Has Roblon appointed a person responsible for Roblon's data ethics work?

1.2 In the past year, has Management adopted a data ethics policy?

1.3 Has the team been called upon to make data ethics assessments and, if so, have these assessments been documented?

1.4 Does the Company consider whether the rights of data subjects are prioritised over the Company's interests (e.g. commercial interests)?

2.1 Does the Company have an up-to-date survey of all instances of personal data processing?

2.2 Have all personal data been processed for a specific, defined purpose?

3.1. Are personal data handed over without instruction?

3.2. Are personal data disclosed without authorisation or without a data ethics assessment?

4.1 Have data ethics assessments been made of new technology commissioned, e.g. machine learning and/or artificial intelligence?

4.2 Is the processing of data transparent to data subjects (are data subjects informed of their data being processed)?

4.4 Has the Company assessed whether data subjects may be given more control of what data are processed?

4.5 Has the Company assessed whether data subjects can get more value from the data processed?

4.6 Has the Company assessed whether the processing of data has any unintended consequences (such as surveillance, spreading of misinformation or the like)?

4.7 Has the Company assessed whether there is a need to protect particular target groups (e.g. children or socially disadvantaged individuals)?

4.8 Does the processing of data result in a general limitation of the rights of data subjects?

4.9 Has the Company considered whether the processing of data may exacerbate social or ethical issues (such as inequality)?

4.10 Are the data ethics principles embedded in the Company's privacy by design procedures?

4.11 Have the Company's privacy by design strategies been communicated to the public?

5.1 Have the employees been instructed in the principles of the data ethics policy?