SimCorp

Data Ethics Policy

December 17, 2021

Data Ethics Policy

1. The purpose of SimCorp's data ethics policy

SimCorp has always taken organizational initiatives to ensure that our activities, products and services are compliant with regulatory requirements for data processing, including the GDPR, and supports our client's compliance with the regulatory requirements they are facing in their activities.

Regulatory compliance, however, is just the beginning. In addition, we wish to ensure a high ethical standard for our data processing in general.

SimCorp's core activity is the development of digital software that enables financial organisations etc. to manage different types of financial data. Our products are offered as 'on-premise' solutions as well as cloud solutions.

Responsible and secure handling of our client's data has always been part of SimCorp's DNA.

We are also aware that the choices we make in relation to the development of our products may indirectly affect individuals and companies, including our clients and our clients' clients, regardless of whether SimCorp processes personal data or not.

Our products are used for the handling of large amounts of financial data and to support our clients' decisions. Errors or inaccuracies or even unintended bias in the design of our systems could have significant socio-economic consequences.

We also process data for our own purposes. We collect and process data on our employees, our clients' employees, our shareholders and partners to administer our relationships and to support our decisions.

It is of great importance to SimCorp that all our departments, employees and partners etc. has a focus on data ethics and ensure that data ethics are embedded in all the above activities, from the very beginning and in every stages of the process.

The purpose of this data ethics policy is to raise awareness of and to enhance SimCorp's data ethical values and their anchoring in our organization. The policy is applicable to all types of data processing, regardless of whether the processing includes personal data. The policy is universal and aims to embrace all scenarios in which data ethics considerations are relevant.

This data ethics policy is addressed to all our employees, our management and the individuals and partners we entrust to carry out activities on our behalf.

2. Data ethical values

Taking into consideration the nature of SimCorp's business activity and our data usage as well as the risks involved, we have identified and created our data ethics policy around the following five fundamental values and principles:

- **Security and integrity**
  We have a high level of security for our own and our partners' data, and we strongly focus on the security in the products we develop. Data must be protected against unauthorized or illegal processing as well as accidental loss, destruction or damage.
- **Transparency**
  We are open and honest with each other and the outside world regarding our usage of data and our motives for our usage, and we demand full transparency from both ourselves and our partners.
- **Accountability and responsibility**
  We act responsibly when we have access to and process data. Our behaviour in relation to data processing and our development of software is characterized by care and caution. We ensure transparency on the organisational responsibility for the development and use of data.

- **Curiosity**
  We are inquisitive and curious and not afraid to ask questions. Curiosity is the source of learning and developing – also when it comes to data ethics.
- **Diversity and equality**
  We promote diversity and equality, and we take diversity and equality into consideration at all relevant stages of the process. Processing of data must never lead to discrimination or produce prejudices about specific groups of the population. We aim to ensure diversity in the development and usage of technology.

3. Data ethical guidelines

The values and principles presented above regulate the general handling of data, including in connection with employment, administration of employees, development of products and storage of our clients' data etc.

Based on a risk-based approach, SimCorp has identified six particularly vital areas of our business giving rise to special attention. For these six areas, we have developed specific guidelines aimed at implementing the five values above in our most vital processes:

3.1 Security measures (Security)

SimCorp develops products and provide services allowing our clients to handle a significant amount of financial data. A large portion of this data is available to and processed by SimCorp. Cybercrime and unauthorized access to this data constitute a severe risk to SimCorp and our clients and to the individuals about whom SimCorp's clients process data. The security surrounding data is therefore crucial.

Security measures must protect against data security breaches and data leaks resulting from external interference, but we must also have internal control measures in place to avoid errors and breaches in connection with our data processing and our development of software etc. We must have documentation containing necessary information on functions, requirements and specifications, background and history of the development of software, so that the necessary information to remedy any future errors, breaches or inaccuracies can be easily retrieved.

In addition, we strive to have clear processes for handling any attacks or threats, which could potentially have an impact on our security and handling of the data available to us.

As part of this work, SimCorp has taken the following measures to ensure a high level of security:

- SimCorp monitors its technical infrastructure to identify and minimize risk to the company's production and operation.
- Established procedures and solutions enable a quick restoration of critical business services.
- SimCorp upholds a high data security level and strict access control to the physical environment and data network.
- Controls are monitored and reviewed to optimize information security.
- SimCorp management and employees are regularly updated on new potential cybercrime threats and how to minimize the risk of phishing and hacking.
- SimCorp has a disaster recovery plan for restoring all critical business services and makes use of state-of-the-art tracing software for detecting unintended access, or attempts, to SimCorp's network.
- The suppliers of this software are diligently screened, using both expert assessments of the product as well as in-house proof of concept.
- SimCorp regularly receives an ISAE 3402 Type 2 report on our third-party service providers, and the hosting providers have undergone substantial successful due diligence performed by SimCorp and its external partners.

- Furthermore, SimCorp has back-to-back agreements with its third-party service providers.
- SimCorp hosting services are audited annually by an external third party, who provides ISAE3402 and SOC assurance reports.

3.2 Open and trusting working environment (Security)

As part of our efforts to ensure a high level of security, we believe it is crucial to have a working environment which is characterized by openness and understanding so that mistakes and errors are not overlooked or neglected.

SimCorp strives to create the framework for such environment by 1) having specific and well-known procedures for the handling of errors, 2) ensuring trust and confidence among employees, management and external parties by creating a safe space for all parties to admit mistakes, and by focusing on solutions and remedy and by 3) focusing on learnings from our mistakes and ensuring that mistakes are not repeated.

In support of this, SimCorp has established a whistleblower system as a means of increasing focus on transparency and to enable reporting on suspected irregularities in the business.

3.3 Artificial intelligence and machine learning (Transparency, diversity and equality)

In recent years, SimCorp has been looking into the potential of using and building solutions supported by artificial intelligence and machine learning. In 2020, we made a breakthrough with streamlining alternatives investments transaction processing by leveraging advanced machine learning technology.

With the use of artificial intelligence and machine learning come new and exciting opportunities allowing us to create more efficient systems and processes. With this, however, also come certain challenges, especially concerning the transparency of the technology and the data on which the system bases its learning.

We therefore aim to have full transparency in our systems, and we demand that our external partners give us full insight into the technology of such products.

Today, SimCorp only uses artificial intelligence and machine learning to a limited extent. As a principle, we only use such products, if 1) the technology of the product is sufficiently transparent and if 2) we do not compromise the principle of diversity and equality by developing or using the product.

3.4 Balancing of interests (Accountability and responsibility)

Before we initiate collection and processing of data, we must identify the interests of all relevant parties and balance opposite interests in order to determine whether the intended processing is legitimate. Data must only be processed if necessary to fulfil the purpose. Before processing, we will always consider whether the purpose of the processing can be achieved in a less intrusive way.

The balancing of interests applies to all types of data, whether it being personal data or not and in all relevant processes, including product development. We therefore endeavour to develop our products with a functionality that allows our clients to process data with a similar approach.

In order to ensure that we can deliver a high level of service with our products, we may collect telemetry data from our clients on their use of our products. Such data is, however, solely processed for the purpose of ensuring that we can provide our clients with the level of service they need and is only collected with prior agreement with the client and with full transparency on our collection and use of the data.

3.5 Evading bias in software development (Diversity and equality)

Operating from 26 locations and counting 68 nationalities among our 2,000 employees, SimCorp is a truly global workplace. SimCorp embraces human individuality and promotes a culture where everyone can be their true selves.

In general, SimCorp does not process data when developing software. However, our clients use our products in the processing of large amount of financial data and to make decisions on investments that eventually concerns individuals. The functionality of our products therefore has a big impact on our clients' data processing. It is thus a core value for SimCorp that our products are built and set up to provide the opportunity to exercise ethical and responsible data processing.

When developing and modifying software, ongoing testing is essential. Which data we use for testing and the way we use this data in machine learning systems can be decisive for the system's functions and decisions, including whether bias occurs. Our system itself does not provide any recommendations for investment decisions but merely allows the end users to make decisions based on a set of objective data.

In the light of the above, we have a focus on evading bias and on ensuring that the data we use is representative and non-discriminatory.

3.6 Awareness and teaching (Curiosity)

It is essential that we create awareness of data ethics across all the countries from which we operate and throughout all employee groups.

It is key that all our employee groups comply with and focus on our data ethics values and guidelines. Therefore, it is mandatory for new employees to participate in a training program on data ethics, just as we make sure to update our employees and management's knowledge of our data ethics policy at annual mandatory courses.

4. Continuous updating of our policy

SimCorp is a company in constant development. As our business develops, our focus points for data ethics may also shift. SimCorp will thus continue to build on and further develop our data ethics policy.

We therefore have ongoing discussions on data ethics and whether we need to amend or update the policy.

In SimCorp, the SVP and General Counsel remains responsible for the Data Ethics Policy and compliance herewith.

This Data Ethics Policy is adopted in Copenhagen on December 17, 2021.

Board of Directors

Peter Schütze

Morten Hübbe

Hervé Couturier

Simon Jeffreys

Adam Warby

Joan A. Binstock

Susan Standiford

Else Braathen

Vera Bergforth

Hugues Chabanis

SimCorp

About SimCorp

SimCorp offers industry-leading, integrated investment management solutions.

Our platform and ecosystem, comprising partners, services, and third-party connectivity empowers us to provide 40% of the world's top 100 financial companies with the efficiency and flexibility needed to succeed.

With over 25 offices around the world, and more than 2,200 employees, we are a truly global, collaborative team that connects every continent and industry seamlessly.

For more information, see www.simcorp.com