AKROS

Akros

Group Outsourcing Policy

Akros Index Engineering Inc.

April 2024

v1.0

First Publication Date: April 11, 2024

Contents

1. Introduction

1.1. Akros Index Engineering Inc. ("AIE" or the "Company") is a wholly owned U.S. subsidiary of Akros Technologies Inc. ("AT").

1.2. AT and its subsidiaries (collectively the "Akros Group") has in place robust governance arrangements which include a clear organizational structure and a framework to identify and to prevent or manage potential conflicts of interest and to ensure that where any judgment or discretion in outsourcing is required, it is independently and honestly exercised.

1.3. This document gives an overview of the main ways in which outsourcing arrangements are identified and managed.

2. Akros Group Outsourcing Policy

2.1. This policy must be followed whenever any of our affiliate's functions or activities are outsourced to third-party service providers. The use of outsourcing arrangements will only be approved if a valid business case for its use is developed. We maintain a *Register of Outsourcing & Contractors Activities*, which contains the names of the external service providers and the services they provide on behalf of our affiliates. The register is available to view upon request.

2.2. Some third-party service providers (to whom we may wish to outsource our services) may be a Data Processor (as defined under the relevant data protection legislation). This will be the case where we transfer client or personnel data to them to process or hold. Anyone instructing a third-party service provider must ensure that they adhere to relevant data transfer policies and procedures.

2.3. Before engaging in any outsourcing agreements, we will undertake the following steps as a baseline requirement:

2.3.1. Assess the data security measures of the external service provider, ensuring they align with pertinent data transfer policies and procedures.

2.3.2. Perform background investigations on the potential services provider, which will include evaluating their technical competencies and reviewing their internal performance standards and monitoring practices.

2.3.3. Conduct a comprehensive risk assessment and implement appropriate measures or safeguards to mitigate any risks identified.

2.4. We only delegate our services to external providers when we are confident that they:

2.4.1. Possess explicit confidentiality and data security policies and are cognizant of our confidentiality data protection, and publicity guidelines.

2.4.2. Implement all necessary measures to safeguard our clients' confidential information.

2.4.3. Commit to adhering to legal and professional responsibilities.

2.4.4. Take all necessary precautions to ensure that their activities do not lead our affiliates to violate these obligations.

2.5. When we have the leverage to set the terms of an outsourcing agreement with a service provider, we will include, at a minimum, the following provisions:

2.5.1. Defined commencement and end dates, with provisions for periodic reviews of the arrangement.

2.5.2. A formal evaluation process that includes procedures enabling our affiliate to effectively monitor the service provider's performance, particularly the quality of their work.

2.5.3. A mechanism for monitoring adherence to our own policies on client care, confidentiality and publicity.

2.5.4. Provisions that allow our affiliates to access and, if necessary, retrieve data and documentation from the service provider.

2.5.5. The requirement of the service provider to ensure the operational security of any data or information and that they comply fully with information security procedures including the maintenance of data confidentiality and data integrity. In particular, the service provider will be required to ensure compliance with our policies on data security and information risk management and that no breach of those policies results from their actions.

2.5.6. The agreement with the service provider includes a commitment to maintain the confidentiality of all client information, stipulating that they will:

2.5.6.1. Ensure that any data transferred to them is kept confidential and is stored and processed securely.

2.5.6.2. Use the data solely for the purposes for which it was provided.

2.5.6.3. Return the data to us (and delete any copies) upon our request, and in any case, not retain the data for longer than six years.

2.5.6.4. Compensate us for any losses or damages resulting from their breach of obligations related to data security and data processing under the outsourcing agreement.

2.5.7. Controls on any further subcontracting or outsourcing by the service provider.

2.5.8. Provisions for the default and termination of the outsourcing arrangement and details regarding the extent of liability for each party.

2.6. Where the service provider will not accept a written agreement or provides services subject to a standard form of contract, this must be reviewed and agreed by the relevant Compliance Officer of each affiliate.

2.7. The Compliance Officer at each affiliate is tasked with managing our Outsourcing Policy. The Compliance Officer is responsible for continuously monitoring all outsourcing agreements and for conducting and documenting a thorough annual evaluation of each arrangement. This evaluation includes assessing compliance with established controls and the quality of work performed.

2.8. Additionally, the Compliance Officer is required to conduct an annual review of this Outsourcing Policy and to regularly examine our *Register of Outsourcing & Contractors Activities* to ensure that our policies and procedures are effectively implemented across our affiliate.

Disclaimer