

## SCHEDULE 6

### SOFTWARE, PORTALS AND DIGITAL TOOLS SERVICES

This Schedule forms an integral part of the Terms & Conditions of Nordic Tax & Accounting OÜ and applies to the use of NTA's own software, accounting systems, client portals, document management systems, digital workflows, electronic communication tools, automation tools, integrations, access credentials, data exports and related digital services provided or made available by NTA.

In the event of a conflict between this Schedule and the General Terms, this Schedule shall prevail for Software, Portals and Digital Tools Services.

#### 1. Scope of this Schedule

1.1. This Schedule applies where NTA provides, uses, grants access to or makes available any software, client portal, accounting system, document management system, online workspace, digital tool, automation, workflow, interface, data room, shared folder, e-mail routing, reporting dashboard or similar digital infrastructure in connection with the Services.

1.2. Such digital tools may be owned, licensed, configured, operated or selected by NTA, or may be provided by third-party vendors selected by NTA.

1.3. NTA may determine, change, replace, suspend, restrict or discontinue the software, portals, systems and digital tools used for the provision of the Services at its discretion, provided that such change does not materially prevent the provision of agreed Services.

1.4. This Schedule does not create any software licence, IT outsourcing agreement, hosting agreement, data storage agreement, escrow arrangement, cybersecurity guarantee or system availability undertaking unless expressly agreed in writing.

#### 2. NTA Systems and Client Access

2.1. NTA may provide the Client with access to selected systems, portals or digital tools solely for the purpose of using the agreed Services.

2.2. Access may be limited, temporary, personal, non-transferable, role-based and subject to identification, authentication, security checks, AML/KYC requirements and payment of all outstanding fees.

2.3. NTA may define user roles, permissions, access levels, upload rights, approval rights, reporting views and available functions.

2.4. The Client has no right to demand access to any internal NTA system, working file, automation, database, template, configuration, source file, source code, workflow, internal note or internal calculation unless expressly agreed in writing.

2.5. NTA may refuse, suspend, restrict or revoke access for security, compliance, non-payment, misuse, termination, technical, operational, AML/KYC, sanctions or risk-related reasons.

#### 3. Client Responsibilities for Access and Users

3.1. The Client is responsible for all users, representatives, employees, contractors and other persons who access NTA systems or digital tools on behalf of the Client.

3.2. The Client shall ensure that only authorised persons access the systems and that all access credentials are kept confidential and secure.

3.3. The Client shall immediately notify NTA of any change in authorised users, employment status, representation rights, security incident, suspected unauthorised access or compromised credentials.

3.4. Any action performed through the Client's user account, authorised user, e-mail address, portal access or credentials may be treated by NTA as an action authorised by the Client.

3.5. The Client shall not share passwords, bypass security controls, create unauthorised users, scrape data, overload systems, reverse engineer tools, introduce malware or use the systems for any purpose other than the agreed Services.

#### 4. Use of NTA Software and Digital Tools

4.1. The Client may use NTA systems and digital tools only in accordance with the agreed scope, NTA's instructions, applicable law and these Terms.

4.2. The Client shall not use NTA systems for unlawful, misleading, abusive, fraudulent, tax evasive, sanctions-related, AML-sensitive, harmful or unauthorised purposes.

4.3. The Client shall not upload false, fabricated, backdated, misleading, unlawful, infected, corrupted or irrelevant documents or data.

4.4. NTA may remove, quarantine, reject or ignore files, data, instructions or uploads that are incomplete, unreadable, suspicious, unlawful, infected, excessive or outside the agreed scope.

4.5. NTA may impose technical limits on file size, storage, access, user numbers, data volume, document volume, API usage, export frequency or similar usage parameters.

#### 5. No Ownership or Transfer of NTA Systems

5.1. All rights in NTA's systems, configurations, workflows, templates, software settings, automation logic, reporting formats, internal structures, methods, databases, know-how and digital infrastructure remain with NTA or the relevant third-party owner.

5.2. The Client does not acquire any ownership, intellectual property right, licence, right of possession, source-code access, system administration right or continuing access right in NTA's systems or digital tools.

5.3. Any access granted to the Client is a limited, revocable, non-exclusive and non-transferable access right for the duration and purpose of the agreed Services.

5.4. Upon termination, suspension or non-payment, NTA may disable access without liability, subject to mandatory law and the agreed handover process.

## **6. Client Data, Uploads and Data Quality**

6.1. The Client remains solely responsible for the accuracy, completeness, legality, authenticity, timeliness and business relevance of all data, files, documents, instructions and uploads provided through NTA systems or digital tools.

6.2. NTA may rely on data uploaded or approved by the Client without independent verification unless expressly agreed otherwise.

6.3. The Client shall ensure that uploaded documents are complete, legible, correctly classified, free from malware, lawfully obtained and suitable for the intended accounting, tax, payroll, corporate or advisory purpose.

6.4. NTA is not liable for errors caused by incorrect file names, duplicate documents, missing attachments, wrong classifications, corrupted files, late uploads, missing approvals, incomplete metadata or inconsistent Client data.

6.5. NTA may require the Client to re-upload, correct, classify, translate, explain or supplement documents and data before NTA processes them.

## **7. Approvals, Electronic Confirmations and Digital Workflows**

7.1. NTA may use electronic approvals, portal approvals, e-mail confirmations, digital signatures, workflow confirmations, status changes, checkboxes and similar electronic methods for instructions and approvals.

7.2. The Client agrees that electronic approvals and confirmations may be treated as valid and binding instructions, approvals and confirmations for the relevant Services.

7.3. The Client shall carefully review all documents, filings, reports, declarations, payroll data, tax calculations, accounting outputs and other materials before approving them electronically.

7.4. If the Client approves a document or workflow step electronically, the Client confirms that the content is accurate, complete, authorised and suitable for the intended purpose.

7.5. NTA is not liable for consequences arising from approvals given by the Client, delayed approvals, missing approvals or approvals given by persons using the Client's credentials or authorised accounts.

## **8. Third-Party Systems and Integrations**

8.1. NTA may use third-party software, cloud services, data storage providers, accounting platforms, document management systems, communication tools, electronic signature tools, OCR tools, automation tools, tax portals, authority portals and other third-party systems in connection with the Services.

8.2. Third-party systems are subject to their own terms, technical limitations, availability, security, updates, outages, errors, support processes and pricing.

8.3. NTA is not liable for failures, downtime, data delays, API errors, bank feed errors, import errors, export errors, synchronisation issues, access restrictions, changed functionality, discontinued services or other issues caused by third-party systems.

8.4. NTA may change third-party providers or workflows where NTA considers this appropriate for operational, security, pricing, compliance, technical or risk-related reasons.

8.5. Additional costs charged by third-party providers may be passed on to the Client where such costs relate to the Client, the Services or the Client's requested functionality.

## **9. Availability, Maintenance and Technical Limitations**

9.1. NTA does not guarantee uninterrupted, error-free or continuous availability of any software, portal, system or digital tool unless expressly agreed in writing.

9.2. Systems may be unavailable due to maintenance, updates, migrations, outages, cybersecurity measures, vendor failures, authority portal downtime, network issues, force majeure or other technical reasons.

9.3. NTA may perform maintenance, updates, changes, security measures and system improvements without prior notice where NTA considers this necessary or appropriate.

9.4. The Client shall maintain its own internet access, devices, browsers, software, e-mail access, authentication tools and technical environment required to use the digital tools.

9.5. NTA is not responsible for the Client's hardware, software, network, browser, e-mail, spam filter, firewall, device security, user training or internal IT environment.

## **10. Cybersecurity and Security Measures**

10.1. NTA may implement security measures, authentication requirements, access controls, monitoring, logging, encryption, IP restrictions, two-factor authentication or other protective measures.

10.2. The Client shall comply with all security requirements notified by NTA and shall ensure that its users do the same.

10.3. NTA may block, suspend or restrict access where NTA suspects unauthorised access, malware, account compromise, misuse, excessive usage, security risk, breach of these Terms or unlawful activity.

10.4. The Client shall immediately notify NTA of any actual or suspected data breach, unauthorised access, phishing incident, malware infection, compromised account or security weakness affecting the Services.

10.5. NTA is not liable for cybersecurity incidents caused by the Client, its users, devices, networks, credentials, negligent handling of access rights or failure to follow security instructions.

## **11. Data Storage, Backups and Archiving**

11.1. NTA may store Client data and documents in systems selected by NTA for the purpose of providing the Services, complying with legal obligations, AML/KYC obligations, accounting rules, tax rules, limitation periods and legitimate administrative purposes.

11.2. NTA may maintain backups, archives, logs and copies in accordance with its internal procedures and legal obligations.

11.3. Unless expressly agreed in writing, NTA does not provide general data backup, disaster recovery, long-term archiving or document custody services for the Client.

11.4. The Client remains responsible for downloading, retaining and backing up documents, reports, filings, outputs, invoices, corporate documents and other information made available to it.

11.5. NTA may delete, archive, restrict or anonymise data after termination or after expiry of applicable retention periods, subject to legal and AML/KYC retention obligations.

## 12. Data Export, Migration and Handover

12.1. Upon termination, the Client may request export or handover of Client data and final work products within the scope required by law and the agreed Services.

12.2. Data export, migration, reconciliation, special formatting, historical reconstruction, bulk download, third-party transfer or handover assistance may be subject to full payment of all outstanding fees and additional service fees.

12.3. Unless expressly agreed, NTA is not obliged to provide data in any specific format, software structure, import template, database dump, source file, editable template or system-specific migration format.

12.4. NTA is not required to provide internal working papers, internal notes, internal review comments, automation logic, templates, system configurations, audit trails or other internal materials.

12.5. NTA may retain copies of exported or handed-over data where required or permitted by law, AML/KYC obligations, tax rules, accounting rules, professional obligations, limitation periods or legitimate business interests.

## 13. Suspension for Non-Payment or Risk

13.1. NTA may suspend or restrict system access, data export, portal access, uploads, downloads, reporting, approvals, workflows, support and related digital functionality if the Client fails to pay any amount when due.

13.2. NTA shall not be liable for missed deadlines, penalties, filings, reporting delays, payroll delays, tax consequences, registry consequences or other losses caused by suspension due to non-payment.

13.3. NTA may also suspend or restrict access for AML/KYC, sanctions, security, misuse, legal, tax, regulatory, operational or reputational risk reasons.

13.4. Reinstatement of access may be subject to full payment of outstanding fees, completion of AML/KYC checks, security review and payment of reactivation or administrative fees.

## 14. Support and User Assistance

14.1. NTA may provide reasonable support for systems and portals used in connection with the Services, within the agreed scope and during NTA's normal business hours.

14.2. Unless expressly agreed, support does not include general IT support, device support, network support, user training, third-party software administration, custom integrations, API development, data cleansing or migration projects.

14.3. Additional support, urgent assistance, repeated user assistance, training, troubleshooting caused by the Client's systems or extensive data correction may be charged separately.

14.4. NTA may require support requests to be submitted through designated channels and may prioritise requests based on urgency, risk, scope, payment status and operational capacity.

## 15. Prohibited Use

15.1. The Client shall not use NTA systems, portals or digital tools to:

- a. upload unlawful, fraudulent, misleading, infected, harmful or irrelevant content;
- b. transmit malware, spam, phishing content or harmful code;
- c. access data of other clients or unauthorised systems;
- d. interfere with the operation, security or integrity of NTA systems;
- e. bypass access controls or authentication mechanisms;
- f. reverse engineer, copy, scrape or reproduce NTA systems, templates or workflows;
- g. conduct unlawful, AML-sensitive, sanctions-related or tax abusive activities;
- h. overload systems or use them outside agreed limits.

15.2. Breach of this clause constitutes a material breach and may result in immediate suspension or termination without liability.

## 16. Confidentiality and Logs

16.1. NTA may maintain system logs, access logs, approval logs, upload records, download records, audit trails, timestamps and other technical records for security, evidentiary, compliance, AML/KYC, operational and service management purposes.

16.2. Such logs may be used by NTA to evidence instructions, approvals, access, uploads, downloads, usage, misuse, security incidents and compliance matters.

16.3. The Client shall keep confidential all access credentials, system links, portal content, NTA workflows, templates, reports, configurations and any non-public information made available through NTA systems.

16.4. NTA may disclose relevant system records to authorities, auditors, lawyers, insurers, IT providers or other parties where required or permitted by law, contract, AML/KYC obligations or legitimate interests.

## 17. Limitation of Liability for Digital Services

17.1. NTA shall not be liable for losses arising from third-party system failures, authority portal downtime, internet

outages, Client IT failures, user errors, incorrect uploads, missing approvals, delayed responses, compromised credentials or misuse of access rights.

17.2. NTA shall not be liable for indirect damage, loss of profit, loss of business opportunity, loss of data caused by the Client, loss of goodwill, loss of financing, loss of access caused by suspension or any consequences of the Client's failure to maintain its own data copies.

17.3. NTA's liability for Software, Portals and Digital Tools Services is subject to the limitation of liability in the General Terms.

17.4. The Client acknowledges that digital tools are support tools for professional services and do not replace the Client's own responsibility for business, tax, accounting, HR, corporate and compliance decisions.

## 18. Fees and Additional Charges

18.1. NTA may charge fees for system access, portal use, user administration, data import, data export, data migration, document storage, OCR processing, additional users, integrations, technical support, training, special reports, custom workflows and other digital services.

18.2. Third-party software costs, licence fees, storage fees, transaction fees, OCR fees, API fees, electronic signature fees, SMS authentication fees or similar costs may be charged to the Client where applicable.

18.3. NTA may require advance payment for software, portal, data migration, setup, integration or customisation work.

18.4. NTA may refuse to perform additional digital or technical work until all fees and third-party costs have been paid.

## 19. Termination and Consequences

19.1. Upon termination of the relevant Services, NTA may disable, restrict or delete the Client's access to portals, systems, dashboards, shared folders, workflows, document spaces and digital tools.

19.2. The Client shall ensure that all necessary documents and outputs are downloaded or requested before termination, subject to payment of all outstanding fees.

19.3. NTA may retain, archive or delete data after termination in accordance with applicable law, AML/KYC obligations, accounting rules, tax rules, limitation periods and internal retention policies.

19.4. NTA is not obliged to maintain live access to systems after termination unless expressly agreed in writing.

19.5. Post-termination assistance, exports, archive retrieval, user reactivation, handover support and data migration may be charged separately.

## 20. Indemnity

20.1. The Client shall indemnify and hold harmless NTA, its management board members, employees, contractors, representatives and affiliated persons against claims, losses, liabilities, penalties, damages, costs and expenses arising out of or in connection with:

- a. misuse of NTA systems, portals or digital tools;
- b. unauthorised access caused by the Client or its users;
- c. incorrect, incomplete, unlawful or infected data uploaded by the Client;
- d. breach of access, security or confidentiality obligations;
- e. instructions or approvals given through the Client's accounts or credentials;
- f. third-party claims arising from the Client's data, documents, users or use of the digital tools;
- g. regulatory, tax, AML/KYC, sanctions or data protection breaches caused by the Client's data, conduct or instructions.

20.2. This indemnity applies in addition to, and not instead of, the limitation of liability and indemnity provisions in the General Terms.

## 21. Survival

21.1. The provisions of this Schedule concerning intellectual property, access records, logs, confidentiality, data retention, limitation of liability, indemnity, fees, prohibited use, data export and post-termination restrictions shall survive termination of the Engagement.