|  |  |
| --- | --- |
| **1. SUPPLIER DETAILS** | |
| Please provide details of the supplier and a POC we can contact for further information if required. | |
| Supplier: | [wflow.com](http://wflow.com) Czech Republic s.r.o. |
| Company address: | Pobřežní 34, 186 00 Praha 8 |
| Contact name: | Filip Dolanský |
| Title: | Product manager |
| E-mail: | [filip.dolansky@wflow.com](mailto:filip.dolansky@wflow.com) |
| Closing Date: | 22.8.2024 |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **2. SERVICE DESCRIPTION** | | | | | |
|  | Questions | Answer/Brief Statement | | | To be added by BDO company |
| SD1 | Provide a brief description of the service and/or products to be provided to the company and/or its customers. | Cloud platform for accounting documents processing. | | |  |
| SD2 | Do the processing activities involve any of the following BDO companies/customer? data types?   * Personal * Source code * Financial   If yes, please describe the relevant data types. | User data and company accounting documents (may include personal information such as e-mail addresses, physical addresses and accounting document data). | | |  |
| SD3 | Do the processing activities include data storage? | Yes  **☐x** | No  **☐** | Data hosted on MS Azure (GDPR compliant), stored in the Netherlands and Ireland concurrently (on-line georeplication). |  |
| SD4 | If the processing activities involve storage of data, in which country or countries will the data be stored? | Data hosted on MS Azure (GDPR compliant), stored in the Netherlands and Ireland concurrently (on-line georeplication). | | |  |
| SD5 | Is it possible to disable this feature to avoid sharing any data? | No | | |  |
| SD6 | If any server locations are added, will it be possible to change locations for ongoing licenses? | No | | |  |
| SD7 | Please provide details of any thirdparty cloud services used in the provision of your service. | MS Azure <https://learn.microsoft.com/en-us/compliance/assurance/assurance-datacenter-security> | | |  |
| SD8 | Describe the format in which the data will be stored or processed  e.g., paper files, media, system data, etc. | No physical media, only meta data and files. | | |  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **3. DATA PROTECTION POLICY AND MANAGEMENT** | | | | | |
|  | Questions | Answer/Brief Statement | | | To be added by BDO company |
| DP1 | Describe the personal data that will be processed on behalf of the BDO company and/or its customers. | User email adresses, organization identification information such as address or VAT number.  All documents and its metadata uploaded by BDO. | | |  |
| DP2 | Describe the data processing activities to be carried out. | Data processed according to the customer settings within the application. | | |  |
| DP3 | Indicate whether the data is about an BDO company/customer intended for transfer to a country or territory outside the European Economic Area. | No | | |  |
| DP4 | Has the data protection policy been documented and implemented by the supplier?  If yes, please provide details of any such policies and procedures [which may be relevant to the service you provide]. | Yes  **☐x** | No  **☐** | ISO 27001 certification As per Microsoft Azure policies |  |
| DP5 | How is the data protection policy communicated to employees? | Following ISO 27001 requirements | | |  |
| DP6 | How will the supplier ensure that employees read and understand their data protection policy? | Following ISO 27001 requirements | | |  |
| DP7 | How often is the data protection policy reviewed and when was it last reviewed? | Following ISO 27001 requirements | | |  |
| DP8 | What measures are in place to assess and report the extent of compliance with the data protection policy? | Following ISO 27001 requirements | | |  |
| DP9 | Are breaches of data protection principles addressed through formal disciplinary procedures? Please provide details. | Yes  **☐x** | No  **☐** | Following ISO 27001 requirements |  |
| DP10 | Has the supplier identified a person who has overall responsibility for data protection compliance? | Yes  **☐x** | No  **☐** | CTO/ Head of development |  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **4. INFORMATION SECURITY POLICY AND MANAGEMENT** | | | | | |
|  | Questions | Answer/Brief Statement | | | To be added by BDO |
| ISP1 | Has the information security policy been documented and implemented by the supplier?  If yes, please provide details of any such policies and procedures [which may be relevant to the service you provide]. | Yes  **☐x** | No  **☐** | Following ISO 27001 requirements |  |
| ISP2 | How is the information security policy communicated to employees? | Following ISO 27001 requirements internal security training | | |  |
| ISP3 | How will the supplier ensure that employees read and understand the information security policy? | Following ISO 27001 requirements | | |  |
| ISP4 | How often is the information security policy reviewed and when was it last reviewed? | Following ISO 27001 requirements, last reviewed in May of 2024 | | |  |
| ISP5 | Has the organization identified an individual who has overall responsibility for information security compliance? | Yes  **☐x** | No  **☐** | CTO/ Head of development |  |
| ISP6 | Is the organization certified to any information security standards (e.g., ISO 27001, PCI/DSS, etc.)?  If yes, please list and provide a copy of each certificate. | Yes  **☐x** | No  **☐** | ISO 27001 |  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **5. HR MANAGEMENT** | | | | | |
|  | Questions | Answer/Brief Statement | | | To be added by BDO |
| HR1 | What checks are carried out during the recruitment process to verify the identity of employees? | Following ISO 27001 requirements,  Background checks | | |  |
| HR2 | Do employment contracts require employees to comply with the company's data protection and information security policies? Please provide details. | Yes  **☐x** | No  **☐** | Following ISO 27001 requirements |  |
| HR3 | What measures are in place to ensure that employees receive adequate training and regular updates on data protection and information security? | Following ISO 27001 requirements | | |  |
| HR4 | Please explain the nature of the training received and any measures taken to reinforce it, e.g., regular reminders on information security procedures. | Following ISO 27001 requirements | | |  |
| HR5 | What measures are in place to ensure that employees processing personal data receive adequate training in relation to the operational duties that they are required to perform? | Following ISO 27001 requirements | | |  |
| HR6 | Are employees required to comply with a NDA covering the period of their employment and beyond? Please provide details. | Yes  **☐x** | No  **☐** | Following ISO 27001 requirements |  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **6. RISK MANAGEMENT** | | | | | |
|  | Questions | Answer/Brief Statement | | | To be added by BDO company |
| RM1 | Has a risk assessment method been adopted to identify and evaluate risks? Please provide details. | Yes  **☐x** | No  **☐** | Following ISO 27001 requirements |  |
| RM2 | Has the supplier documented and implemented a disaster recovery or security breach policy?  If yes, please provide details of any such policies and procedures [which may be relevant to the service you provide]. | Yes  **☐x** | No  **☐** | Following ISO 27001 requirements |  |
| RM3 | Does the risk assessment process consider the harm likely to result from a security breach? Please describe. | Yes  **☐x** | No  **☐** | Following ISO 27001 requirements |  |
| RM4 | Does the risk assessment process assess the realistic likelihood of a security failure occurring (given the prevailing threats and vulnerabilities)? Please describe. | Yes  **☐x** | No  **☐** | Following ISO 27001 requirements |  |
| RM5 | Does the risk assessment estimate risk levels and what is acceptable? Please describe. | Yes  ☐**x** | No  ☐ | Following ISO 27001 requirements |  |
| RM6 | Is there a process in place to identify and evaluate risk treatment options? Please provide details. | Yes  **☐x** | No  **☐** | Following ISO 27001 requirements |  |
| RM 7 | Is there a process in place to select controls to mitigate unacceptable levels of risk? Please provide details. | Yes  **☐x** | No  ☐ | Following ISO 27001 requirements, <https://docs.microsoft.com/en-us/compliance/assurance/assurance-datacenter-security> |  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **7. PHYSICAL SECURITY** | | | | | |
|  | Questions | Answer/Brief Statement | | | To be added by BDO company |
| DS1 | List all physical locations from which the proposed services are to be provided to the BDO company and/or its customers. | <https://docs.microsoft.com/en-us/compliance/assurance/assurance-datacenter-security>  Data hosted on MS Azure (GDPR compliant), located in the Netherlands and Ireland concurrently (on-line georeplication). | | |  |
| DS2 | Identify the activities (relevant to the provision of services to the BDO company and/or its customers) that are carried out at each of the above locations. | <https://docs.microsoft.com/en-us/compliance/assurance/assurance-datacenter-security>  Data hosted on MS Azure (GDPR compliant), located in the Netherlands and Ireland concurrently (on-line georeplication). | | |  |
| DS3 | Describe the physical access controls (e.g., door locks, badge/electronic key ID, etc.) that prevent unauthorized access to the facilities. | <https://docs.microsoft.com/en-us/compliance/assurance/assurance-datacenter-security> | | |  |
| DS4 | Is access to these sites through an adequately guarded reception desk? | Yes  ☐ | No  ☐ | <https://docs.microsoft.com/en-us/compliance/assurance/assurance-datacenter-security> |  |
| DS5 | Is there a 24-hour security service present at these locations? | Yes  ☐ | No  ☐ | <https://docs.microsoft.com/en-us/compliance/assurance/assurance-datacenter-security> |  |
| DS6 | Have monitored alarms been installed at these locations to detect unauthorized entry outside of business hours? | Yes  **☐** | No  ☐ | <https://docs.microsoft.com/en-us/compliance/assurance/assurance-datacenter-security> |  |
| DS7 | If monitored alarms have been installed, explain who monitors them and describe response procedures. | <https://docs.microsoft.com/en-us/compliance/assurance/assurance-datacenter-security> | | |  |
| DS8 | Do these sites have automated access control systems in place? | Yes  ☐ | No  **☐** | <https://docs.microsoft.com/en-us/compliance/assurance/assurance-datacenter-security> |  |
| DS9 | Do access control systems record the entry/exit of personnel and, if so, how long is this information retained? | Yes  ☐ | No  **☐** | <https://docs.microsoft.com/en-us/compliance/assurance/assurance-datacenter-security> |  |
| DS10 | Has camera equipment been installed at these locations to prevent and detect unauthorized or illegal activities? | Yes  **☐** | No  ☐ | <https://docs.microsoft.com/en-us/compliance/assurance/assurance-datacenter-security> |  |
| DS11 | Are the cameras monitored? | Yes  ☐ | No  ☐ | <https://docs.microsoft.com/en-us/compliance/assurance/assurance-datacenter-security> |  |
| DS12 | How long are camera images kept and who has access to the recorded material? | <https://docs.microsoft.com/en-us/compliance/assurance/assurance-datacenter-security> | | |  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **8. TECHNICAL SECURITY** | | | | | |
|  | Questions | Answer/Brief Statement | | | To be added by BDO company |
| TS1 | Where will the servers be located that will carry the data of the BDO company and/or its customers? | <https://docs.microsoft.com/en-us/compliance/assurance/assurance-datacenter-security> | | |  |
| TS2 | Describe how the BDO company data and/or its customer data will be logically separated from the customer data of other suppliers. | All customers data are separated by application logic within single databaze instance. Binary data (files) are physically separated in the storage. | | |  |
| TS3 | Describe the technical security controls deployed to prevent unauthorised access to the BDO company/customer data, e.g., use of unique IDs and passwords, access rights granted only to members of management, etc. | All customers data are separated by application logic within single databaze instance. Binary data (files) are physically separated in the storage. Only the authorized users can access the relevant data. | | |  |
| TS4 | Are the servers on which the BDO company and/or its data will reside monitored to detect unauthorized access or security breaches?  Please provide details. | Yes  **☐** | No  **☐** | <https://docs.microsoft.com/en-us/compliance/assurance/assurance-datacenter-security> |  |
| TS5 | If applicable, describe any technical security controls deployed to protect the BDO company and/or customer data during transfer. | All communication between the server and client is secured by TLS/SSL, i.e. HTTPS protocols, and is certified by Microsoft CA.Microsoft Azure servers use the 256-bit Advanced Encryption Standard (AES) for encrypting data. | | |  |
| TS6 | Is a portable device such as laptops etc. used to store the BDO company data and/or its customer data and therefore is the data held on that device encrypted to prevent unauthorised access? Please provide details. | Yes  **☐** | No  **☐x** |  |  |
| TS7 | Are penetration tests regularly carried out to identify weaknesses and vulnerabilities in the IT infrastructure? If so, when was the last test held and were any problems found? | Yes  **☐x** | No  **☐** | 2Q2023, next one is planned on 4Q2024. No major security issues found |  |
| TS8 | In terms of vulnerability patching, what process do you use to ensure your data processing equipment is protected with the latest software updates and patches? | Following ISO 27001 requirements | | |  |
| TS9 | Indicate whether anti-virus software has been deployed to protect your IT infrastructure. Please provide details on how it is updated. | Yes  **☐** | No  **☐** | Following ISO 27001 requirements |  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **9. OPERATIONAL MANAGEMENT** | | | | | |
|  | Questions | Answer/Brief Statement | | | To be added by BDO company |
| OM1 | What procedures are in place to ensure that information (e.g., paper documents and data) is securely and permanently destroyed or deleted when no longer required or when equipment is replaced? | Following ISO 27001 requirements | | |  |
| OM2 | Will the destruction of the BDO. company data/customer data be performed by a third party, and if so, is there a contract with that third party? | Yes  ☐ | No  ☐**x** |  |  |
| OM3 | Indicate whether the contract requires the third party to ensure an adequate level of data protection and describe how this is checked/verified. |  | | |  |
| OM4 | Are certificates of destruction provided by the third party to confirm that the information has been securely stored/destroyed? If not, please indicate what other evidence of destruction is provided. | Yes  ☐ | No  ☐ |  |  |
| OM5 | Has a clear policy been put in place to ensure confidentiality and availability of data? How is this monitored and enforced? | Yes  ☐ | No  ☐ | Following ISO 27001 requirements |  |
| OM6 | Is the management of removable computer media such as tapes, disks, CDs/DVDs, cassettes and USB drives controlled? Please provide more detailed on-site controls. | Yes  ☐ | No  ☐ | No physical media used |  |
| OM7 | What measures have been put in place to ensure that removable media is handled properly and disposed of safely and securely when no longer needed? | No physical media used | | |  |
| OM8 | Are regular system backups performed and if so, how often? | Yes  ☐**x** | No  ☐ | * Database mirroring in real time in a replicated copy that is located in a secondary geo-location. - Database backup is done to geo-redundand backup storage, has a retention of 7 days and is set as follows: • Complete backups every week • Differential backups every 24 hours • Backups of transaction log every 10 minutes - Storage files mirroring in real time in a replicated copy that is located in a secondary geo-location. - At the organization level, the user can set up automatic backup of their data. Data (metadata and attached files) are stored in the form of an organization compressed file in the form of a compressed file. Backup is incremental and is performed daily at night." |  |
| OM9 | Where are the backups stored? If they are stored off-site, are they encrypted? Are they provided with an adequate level of protection? Please provide details. | * Database mirroring in real time in a replicated copy that is located in a secondary geo-location. - Database backup is done to geo-redundand backup storage, has a retention of 7 days and is set as follows: • Complete backups every week • Differential backups every 24 hours • Backups of transaction log every 10 minutes - Storage files mirroring in real time in a replicated copy that is located in a secondary geo-location. - At the organization level, the user can set up automatic backup of their data. Data (metadata and attached files) are stored in the form of an organization compressed file in the form of a compressed file. Backup is incremental and is performed daily at night." | | |  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **10. SUBCONTRACTORS** | | | | | |
|  | Questions | Answer/Brief Statement | | | To be added by BDO company |
| SC1 | Will any aspect of the service to be provided to the BDO company and/or its customers be outsourced to a third party? | Yes  ☐**x** | No  ☐ | ROSSUM Dativery |  |
| SC2 | Provide the names and addresses of all subcontractors who will be involved in providing services to the BDO company and/or its customers. | ROSSUM: <https://drive.google.com/file/d/1aW1Lt4pv5pplG1OSfDhMmSPnprvqKZ9z/view>  Dativery: <https://www.dativery.com/cs/spolecnost/terms/> | | |  |
| SC3 | Indicate whether subcontracting services are to be provided from a country or territory outside the European Economic Area. If yes, please specify the country/countries. | Yes  ☐ | No  ☐**x** |  |  |
| SC4 | Are subcontractors subject to written contracts with the supplier that include provisions on data protection and information security? | Yes  ☐**x** | No  ☐ |  |  |
| SC5 | What processes are in place to ensure that subcontractors comply with data protection and information security obligations? | Written contracts. | | |  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **11. BUSINESS CONTINUITY MANAGEMENT** | | | | | |
|  | Issues/aspects examined | Answer/Brief supporting statement | | | To be added by BDO company |
| BC1 | Are contingency plans in place for the timely maintenance and/or recovery of business operations following interruption or failure of critical business processes? | Yes  ☐**x** | No  ☐ | <https://docs.microsoft.com/en-us/compliance/assurance/assurance-datacenter-security> |  |
| BC2 | Do these plans include the provision of restoration of services to the BDO company and/or its customers?  Please provide details. | Yes  ☐**x** | No  ☐ | <https://docs.microsoft.com/en-us/compliance/assurance/assurance-datacenter-security> |  |
| BC3 | Are these plans regularly tested and maintained to ensure they are up-to-date and effective? | Yes  ☐**x** | No  ☐ | <https://docs.microsoft.com/en-us/compliance/assurance/assurance-datacenter-security> |  |
| BC4 | When were these plans last tested and were any problems found? |  | | |  |
|  | Have there been any data breaches or other privacy concerns within your organisation in the last 12 months?  If yes, please give a brief description of the incident, the action taken and the outcome. | Yes  ☐ | No  ☐**x** |  |  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **12. COMPANY STABILITY** | | | | | |
|  | Questions | Answer/Brief Statement | | | To be added by BDO company |
| CS1 | In the context of the proposed business commitment, please provide an explanation of why you think you are financially suitable. |  | | |  |
| CS2 | Do you have the necessary finances to meet your obligations for the duration of the potential contract? | Yes  ☐**x** | No  ☐ |  |  |
| CS3 | Does your company have professional indemnity insurance in place? If yes, please provide details. | Yes  ☐**x** | No  ☐ |  |  |
| CS4 | Have there been any professional liability claims against the company, a partner or director or their predecessors in the last 6 years?  If yes, please give details of the year(s) in which the claim(s) was made, the amount paid and/or outstanding and briefly the circumstances surrounding the claim(s) and/or circumstances. Use a separate sheet if necessary. | Yes  ☐ | No  ☐**x** |  |  |

|  |  |
| --- | --- |
| **13. CHECKLIST** | |
| Before returning the questionnaire, use this checklist to confirm that you have provided all the information requested. | |
| **☐** | Information about the supplier and contact details of the respondent are set out in Section 1. |
| **☐** | All relevant questions have been answered. Questions that are not relevant have been marked that way and a brief explanation has been provided as to why they are not relevant. |
| ☐ | A copy of the supplier's information security certificate(s) was provided with the completed questionnaire. |