Review of the current situation

Key questions for our organisation

# To be filled in by the internal IT/OT department:

|  |  |
| --- | --- |
| Supplier name: |  |
| Service provided by the supplier: |  |
| Contact person within our organisation: |  |
| Contact: |  |
| Questionnaire No: |  |

# Services provided by the supplier

| 1.1 | Are the services that the supplier or partner provides to us an important part of our business processes? | Yes  No  I don’t know |
| --- | --- | --- |
|  | Please describe the services. |  |

# IT/OT products provided by the supplier

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 2.1 | Does the supplier provide us with IT or OT products that run on our (critical) systems? | | Yes ☐  No ☐  I don’t know ☐ | |
|  | | Please describe the IT/OT products. |  |

# Supplier access to internal systems

| 3.1 | Does the supplier have access to our (critical) systems? | Yes ☐  No ☐  I don’t know ☐ |
| --- | --- | --- |
|  | If your answer is 'yes', please specify the type of data that is stored in these systems. |  |
|  | Internal data about our organisation | Yes ☐  No ☐  I don’t know ☐ |
|  | Internal business data, including information about our organisation's customers or partners | Yes ☐  No ☐  I don’t know ☐ |
|  | Data about our organisation's employees | Yes ☐  No ☐  I don’t know ☐ |
|  | Personal data about our organisation's customers / partners | Yes ☐  No ☐  I don’t know ☐ |
|  | Identification data (passwords) of our organisation's employees | Yes ☐  No ☐  I don’t know ☐ |
|  | Other: |  |
| 3.2 | If applicable: Were the supplier's employees background checked before they were given access to computer systems that operate within our organisation's IT networks or computer systems that process our organisation's data? | Yes ☐  No ☐  I don’t know ☐ |
|  | If your answer is 'no', please adjust the contract's 'Assignment of rights' section accordingly. |  |

# Systems operated by the supplier

| 4.1 | Does the supplier operate systems for us that we need for critical business processes? For example, SaaS applications for recruitment, payroll or collaboration? | | Yes ☐  No ☐  I don’t know ☐ |
| --- | --- | --- | --- |
| 4.2 | | What data is collected or stored? |  |
|  | | Personal data (e.g. surname, first name, date of birth, place of birth, OASI number, passport or ID number, address, telephone number, email address, IP addresses). | Yes ☐  No ☐  I don’t know ☐ |
|  | | Sensitive personal data[[1]](#footnote-1) (e.g. information on health, religion, politics or ideology, sexual orientation, information to do with the private sphere, biometric and genetic information, criminal prosecution records, in accordance with the Swiss Data Protection Act). | Yes ☐  No ☐  I don’t know ☐ |
|  | | Credit card data | Yes ☐  No ☐  I don’t know ☐ |
|  | | Connection data (e.g. IP addresses, geolocation, GPS position data, other telemetry data). | Yes ☐  No ☐  I don’t know ☐ |

# Cyberattacks on the supplier

These questions are relevant if the supplier's services affect our business processes or if the supplier processes data on our behalf.

| 5.1 | In the event of a serious cyberattack on the supplier, can our organisation ensure that there will be no loss of data? | Yes ☐  No ☐  I don’t know ☐ |
| --- | --- | --- |
|  | If your answer is 'no', please describe our organisation's procedure for such an event (e.g. isolation / access monitoring / MFA). |  |

| 5.2 | Could we continue to operate if our supplier were unavailable (for an extended period of time)? | Yes ☐  No ☐  I don’t know ☐ |
| --- | --- | --- |
|  | If your answer is 'no', please describe our organisation's procedure for such an event (e.g. how would we deal with an outage / what is our emergency plan / offline backups): |  |
| 5.3 | Would we be able to continue to provide our services if our supplier were to become unavailable (for an extended period of time)? | Yes ☐  No ☐  I don’t know ☐ |
|  | If your answer is 'no', please describe our organisation's procedure for such an event (e.g. how would we deal with an outage / what is our emergency plan): |  |

1. 'Sensitive personal data' is any data which, if published, could create a high risk for the people concerned. [↑](#footnote-ref-1)