

Technical and organizational measures

A. Measures for the assurance of confidentiality and integrity

1.	Measures of access control related to the server rooms
1.0	Are personal data stored on servers that are operated by you? <input checked="" type="checkbox"/> yes <input type="checkbox"/> no
	If 1.0 no: In this case the further questions under A1 <u>do not</u> need to be answered. Continue to A2. Furthermore, questions B1 and B2 also do not require an answer.
1.1	Location of the server room / data center (DC) Diesbach, Switzerland Click here to insert text.
1.2	Are the personal data stored in more than one server location / data center? (i.e. on back up servers, cloud services)? <input type="checkbox"/> yes <input checked="" type="checkbox"/> no
1.3	If 1.2 yes: Please also fill out the appropriate details of the further locations. Further server locations: Click here to insert text.
1.4	Does the following information regarding access control measures apply to all server locations / data centers in use? <input checked="" type="checkbox"/> yes <input type="checkbox"/> no
1.5	If 1.4 no: Please answer questions 1.6 to 1.21 and section B for further locations.
1.6	Is the server room windowless? <input type="checkbox"/> yes <input checked="" type="checkbox"/> no
1.7	If 1.6 no: How are the windows protected from burglary? <input type="checkbox"/> barred <input type="checkbox"/> alarmed <input checked="" type="checkbox"/> lockable <input type="checkbox"/> not at all <input type="checkbox"/> Other: Please specify
1.8	Is the server room secured by an alarm system? <input type="checkbox"/> yes <input checked="" type="checkbox"/> no
1.9	If 1.8 yes: Who is informed if the alarm system is triggered? Multiple answers possible! <input type="checkbox"/> Commissioned security firm <input type="checkbox"/> Administrator <input type="checkbox"/> IT manager <input type="checkbox"/> Other: please specify
1.10	Is the server room under video surveillance? <input type="checkbox"/> yes, without image recording <input checked="" type="checkbox"/> yes, with image recording <input type="checkbox"/> no
1.11	If 1.10 yes, with image recording: How long is the video footage stored? please insert a value in days <input type="text" value="1"/> days
1.12	How many people have access to the server room and which functions do they have? Number of persons: please specify <input type="text" value="3"/> Role in the company: please specify the role of the relevant persons in the company <input type="text" value="Devops and datacenter engineers"/>
1.13	Is there an electronic lock system in place in the server room? <input type="checkbox"/> yes <input checked="" type="checkbox"/> no, there is a mechanical lock
1.14	If 1.13 yes: Which entry technology is in use? Multiple answers possible! <input type="checkbox"/> RFID <input type="checkbox"/> PIN <input type="checkbox"/> Biometrics <input type="checkbox"/> Other: please specify

1.1 5	If 1.13 yes: Are access rights assigned individually? <input type="checkbox"/> yes <input type="checkbox"/> no
1.1 6	If 1.13 yes: Will accesses to the server room be logged in the access system? <input type="checkbox"/> yes, successful as well as unsuccessful attempts <input type="checkbox"/> yes, but only successful accesses <input type="checkbox"/> yes, but only unsuccessful attempts <input type="checkbox"/> no, the lock will only be released or not.
1.1 7	If 1.16 is yes: For how long will access data be stored before erasure? Please insert value in days days
1.1 8	If 1.13 no: how many keys to the server room exist, where are they stored and who distributes them? Number of keys: Number of keys Storage location: Insert storage location Person responsible for distributing keys: please specify
1.1 9	What is the access door to the server room made of? <input type="checkbox"/> Steel / Metal <input checked="" type="checkbox"/> Other material
1.2 0	Is the server room being used for other purposes besides its actual function? <input type="checkbox"/> yes <input checked="" type="checkbox"/> no
1.2 1	If 1.20 yes: What else is kept in the server room? <input type="checkbox"/> Telephone system <input type="checkbox"/> Storage of stationery <input type="checkbox"/> Storage of files <input type="checkbox"/> Archive <input type="checkbox"/> Storage of IT equipment <input type="checkbox"/> Other: please specify
	In your opinion, are the documented measures appropriate, given the state of the art, implementation costs, nature, scope, context and purposes of the processing as well as the likelihood and severity of the risk for the rights and freedoms of the data subject, such that an appropriate standard of protection is guaranteed? <input checked="" type="checkbox"/> Appropriate <input type="checkbox"/> Appropriate with reservations <input type="checkbox"/> Inappropriate Reasons:
2.	Access control measures to the office rooms
2.1	Location(s) of the client workstations, from which personal data are accessed: Please specify location Worldwide
2.2	Is there a porter service / a constantly occupied lobby area to the building / to the office? <input type="checkbox"/> yes <input checked="" type="checkbox"/> no
2.3	Is a visitor's book implemented? <input type="checkbox"/> yes <input checked="" type="checkbox"/> no
2.4	Is the building or is the office protected by a burglar alarm? <input type="checkbox"/> yes <input checked="" type="checkbox"/> no

2.5	<p>If 2.4 yes: Who is informed if the alarm system is triggered? Multiple answers possible!</p> <p><input type="checkbox"/> Commissioned security firm <input type="checkbox"/> Administrator <input type="checkbox"/> IT manager <input checked="" type="checkbox"/> Other: please specify The power plant & site management team</p>
2.6	<p>Is the office building or its entrances under video surveillance?</p> <p><input checked="" type="checkbox"/> yes, without image recording <input type="checkbox"/> yes, with image recording <input type="checkbox"/> no</p>
2.7	<p>If 2.6 yes, with image recording: For how long is the video footage stored? please insert a value in days days</p>
2.8	<p>Are the building / office rooms secured with an electronic lock system?</p> <p><input type="checkbox"/> yes, building and office rooms are electronically locked</p> <p><input type="checkbox"/> yes, but only the building, not the entrance to the office or to the story that the office is on</p> <p><input type="checkbox"/> yes, but only the entrance to the office / the story that the office is on, not the entire building</p> <p><input checked="" type="checkbox"/> no</p>
2.9	<p>If 2.8 yes: Which entry technology is in use? Multiple answers possible!</p> <p><input type="checkbox"/> RFID <input type="checkbox"/> PIN <input type="checkbox"/> Biometrics <input type="checkbox"/> Other: please specify</p>
2.1 0	<p>If 2.8 yes: Are access rights assigned individually?</p> <p><input type="checkbox"/> yes <input type="checkbox"/> no</p>
2.1 1	<p>If 2.8 yes: Will accesses to the server room be logged in the access system?</p> <p><input type="checkbox"/> yes, successful as well as unsuccessful attempts</p> <p><input type="checkbox"/> yes, but only successful accesses</p> <p><input type="checkbox"/> yes, but only unsuccessful attempts</p> <p><input type="checkbox"/> no, the lock will only be released or not.</p>
2.1 2	<p>If 2.11 yes: For how long will access data be stored before deletion? Please insert value in days days</p>
2.1 3	<p>If 2.11 yes: Are the records regularly assessed?</p> <p><input type="checkbox"/> yes <input type="checkbox"/> no, but assessment would be possible if required</p>
2.1 4	<p>Is there a mechanical lock for the building / office rooms?</p> <p><input checked="" type="checkbox"/> yes <input type="checkbox"/> no</p>
2.1 5	<p>If 2.14 yes: Is the key distribution recorded, who distributes them?</p> <p><input checked="" type="checkbox"/> yes <input type="checkbox"/> no Responsible person: Please specify The power plant & site management team</p>
2.1 6	<p>Are there official access regulations for visitors to the premises?</p> <p><input type="checkbox"/> no</p> <p><input checked="" type="checkbox"/> yes, visitors will be received at the entrance / reception by the contact person and must be accompanied at all times</p>
	<p>In your opinion, are the documented measures appropriate, given the state of the art, implementation costs, nature, scope, context and purposes of the processing as well as the likelihood and severity of the risk for the rights and freedoms of the data subject, such that an appropriate standard of protection is guaranteed?</p> <p><input checked="" type="checkbox"/> Appropriate <input type="checkbox"/> Appropriate with limitations <input type="checkbox"/> Inappropriate</p> <p>Reason:</p>

3	Access control measures to the system
3.1	<p>Is there a process for the distribution of access information (e.g. user names) and access rights for newly instated / removal of access information for departing employees, or for organizational changes?</p> <p><input checked="" type="checkbox"/> Defined distribution process</p> <p><input type="checkbox"/> No defined distribution process, on demand</p> <p><input type="checkbox"/> Other: please specify</p>
3.2	<p>Is assigning or changing the access information recorded?</p> <p><input checked="" type="checkbox"/> yes <input type="checkbox"/> no</p>
3.2	<p>Do employees log in via an individual authorization in the central directory service?</p> <p><input checked="" type="checkbox"/> yes <input type="checkbox"/> no</p>
3.3	<p>Are binding password parameters in operation?</p> <p><input type="checkbox"/> yes <input checked="" type="checkbox"/> no</p>
3.4	<p>Password character length: please insert unlimited</p> <p>Do the password need to contain special characters?</p> <p><input type="checkbox"/> yes <input checked="" type="checkbox"/> no</p> <p>Expiration period in days: please insert unlimited</p>
3.5	<p>Does the IT system enforce all users to comply with the above-mentioned password requirements?</p> <p><input checked="" type="checkbox"/> yes <input type="checkbox"/> no</p>
3.6	<p>Is there an automatic screen lock after a defined length of inactivity? Yes</p> <p>If yes, after how many minutes? variable</p> <p>please insert value in minutes minutes</p>
3.7	<p>What measures are taken when a password is lost, forgotten or compromised?</p> <p><input checked="" type="checkbox"/> Admin issues a new initial password</p> <p><input type="checkbox"/> None</p>
3.8	<p>Is there a limited amount of unsuccessful log in attempts that can be made?</p> <p><input checked="" type="checkbox"/> yes, Please specify number attempts <input type="checkbox"/> no</p> <p>Software defined</p>
3.9	<p>If 3.8 yes, How long will access be denied, when the maximum number of unsuccessful attempts have been made?</p> <p><input type="checkbox"/> Access will be revoked until it is manually reinstated software defined</p> <p><input checked="" type="checkbox"/> Access will remain locked for Please insert value in minutes minutes</p>
3.10	<p>How does authentication occur by remote accesses?</p> <p><input checked="" type="checkbox"/> Token <input checked="" type="checkbox"/> VPN-Certificate <input checked="" type="checkbox"/> Password</p>
3.11	<p>Is there a limited amount of unsuccessful log in attempts that can be made remotely?</p> <p><input checked="" type="checkbox"/> yes, Please specify number attempts <input type="checkbox"/> no</p> <p>software defined</p>

3.12	<p>How long will access be denied, when the maximum number of unsuccessful attempts have been made?</p> <p><input type="checkbox"/> Access will be revoked until it is manually reinstated software defined</p> <p><input checked="" type="checkbox"/> Access will remain locked for Please insert value in minutes minutes</p>
3.13	<p>Is the remote access disconnected after a defined period of inactivity?</p> <p><input type="checkbox"/> yes, after Please insert value in minutes minutes <input checked="" type="checkbox"/> no</p>
3.15	<p>Are the systems that process personal data secured by a firewall?</p> <p><input checked="" type="checkbox"/> yes <input type="checkbox"/> no</p>
3.16	<p>If 3.15 yes: Is the firewall updated regularly?</p> <p><input checked="" type="checkbox"/> yes <input type="checkbox"/> no</p>
3.17	<p>If 3.15 yes: Who administers the firewall?</p> <p><input checked="" type="checkbox"/> Own IT department <input type="checkbox"/> External service provider</p>
3.18	<p>If an external service provider is in use: Can the firewall be intruded upon without surveillance by the IT department?</p> <p><input type="checkbox"/> yes <input type="checkbox"/> no, intrusion is only possible following the four-eyes principle with an employee of IT</p>
	<p>In your opinion, are the documented measures appropriate, given the state of the art, implementation costs, nature, scope, context and purposes of the processing as well as the likelihood and severity of the risk for the rights and freedoms of the data subject, such that an appropriate standard of protection is guaranteed?</p> <p><input checked="" type="checkbox"/> Appropriate <input type="checkbox"/> Appropriate with limitations <input type="checkbox"/> Inappropriate</p> <p>Reasons:</p>
4	Measures for the assurance of paper documents, mobile data carriers and mobile devices
4.1	<p>How are redundant documents containing personal information (e.g. printouts / files / correspondence) disposed of?</p> <p><input type="checkbox"/> wastepaper / residual waste</p> <p><input type="checkbox"/> shredders, the use of which is advised</p> <p><input type="checkbox"/> Documents are stored in securely locked disposal bin and sent to certified disposal service provider for destruction.</p> <p><input checked="" type="checkbox"/> Other: please specify Customer personal data are not printed out and handled only digitally</p>
4.2	<p>How are redundant data media containing personal information (e.g. USB sticks, hard disks) disposed of?</p> <p><input type="checkbox"/> physical destruction by internal IT department</p> <p><input type="checkbox"/> physical destruction by an external service provider</p> <p><input type="checkbox"/> Deletion of data by please insert number overwrites</p> <p><input checked="" type="checkbox"/> Other: please specify Disk encryption</p>

4.3	<p>Are mobile data carriers permitted (e.g. USB sticks)?</p> <p><input checked="" type="checkbox"/> yes <input type="checkbox"/> no</p>
4.4	<p>Can employees use their own personal data carriers (e.g. personal USB sticks)?</p> <p><input type="checkbox"/> in general, yes</p> <p><input type="checkbox"/> yes, but only after authorization and assessment of the storage device by the IT</p> <p><input checked="" type="checkbox"/> no, all necessary storage devices are issued by the company</p>
4.6	<p>Are personal data encrypted on mobile devices?</p> <p><input type="checkbox"/> Encrypted hard drive</p> <p><input type="checkbox"/> Encryption of individual processes</p> <p><input checked="" type="checkbox"/> No measures</p>
4.7	<p>Do employees process personal data on their own private devices (bring your own device)?</p> <p><input type="checkbox"/> yes <input checked="" type="checkbox"/> no</p>
<p>In your opinion, are the documented measures appropriate, , given the state of the art, implementation costs, nature, scope, context and purposes of the processing as well as the likelihood and severity of the risk for the rights and freedoms of the data subject, such that an appropriate standard of protection is guaranteed?</p> <p><input checked="" type="checkbox"/> Appropriate <input type="checkbox"/> Appropriate with limitations <input type="checkbox"/> Inappropriate</p> <p>Reasons:</p>	
<p>5 Measures for secure data transfer</p>	
5.1	<p>Are data transfers continually encrypted?</p> <p><input type="checkbox"/> no at all</p> <p><input type="checkbox"/> no, data transfer only per mpls</p> <p><input type="checkbox"/> only individually</p> <p><input type="checkbox"/> an encrypted file as a mail attachment</p> <p><input type="checkbox"/> via PGP/SMime</p> <p><input type="checkbox"/> via an encrypted data carrier</p> <p><input checked="" type="checkbox"/> via VPN</p> <p><input checked="" type="checkbox"/> via https/TLS</p> <p><input checked="" type="checkbox"/> via SFTP</p> <p><input type="checkbox"/> Other: please specify</p>

5.2	<p>Who administers the keys / certificates?</p> <p><input checked="" type="checkbox"/> Administrator themselves <input type="checkbox"/> Internal IT <input type="checkbox"/> External service provider</p>
5.2	<p>Will data transfers be documented?</p> <p><input type="checkbox"/> yes <input checked="" type="checkbox"/> no</p>
5.3	<p>If 5.2 yes: How long can recorded data be stored?</p> <p>please insert value in days days</p>
5.4	<p>If 5.2 yes: Are records regularly assessed?</p> <p><input type="checkbox"/> yes <input type="checkbox"/> no, but an assessment would be possible if required</p>
	<p>In your opinion, are the documented measures appropriate, given the state of the art, implementation costs, nature, scope, context and purposes of the processing as well as the likelihood and severity of the risk for the rights and freedoms of the data subject, such that an appropriate standard of protection is guaranteed?</p> <p><input checked="" type="checkbox"/> Appropriate <input type="checkbox"/> Appropriate with reservations <input type="checkbox"/> Inappropriate</p> <p>Justification:</p>

B. Measures for the assurance of availability

1.	Server rooms
1.1	Does the server room have a fireproof / fire-resisting access door? <input checked="" type="checkbox"/> yes <input type="checkbox"/> no
1.2	Is the server room fitted with smoke detectors? <input type="checkbox"/> yes <input checked="" type="checkbox"/> no
1.3	Is the server room connected to a fire alarm control panel? <input type="checkbox"/> yes <input checked="" type="checkbox"/> no
1.4	Is the server room fitted with extinguishing systems? Multiple answers possible! <input type="checkbox"/> yes, CO2 extinguishers <input type="checkbox"/> yes, Halon / Argon extinguishing system <input checked="" type="checkbox"/> others: foam please specify
1.5	What are the external walls of the server rooms made of? <input checked="" type="checkbox"/> solid wall (e.g. concrete) <input type="checkbox"/> lightweight construction <input type="checkbox"/> Fireproof wall (e.g. F90)
1.6	Is the server room air-conditioned? <input type="checkbox"/> yes <input checked="" type="checkbox"/> no
1.7	Does the server room have an uninterruptible power supply (UPS)? <input checked="" type="checkbox"/> yes <input type="checkbox"/> no
1.8	Is the power supply to the server room also ensured via a diesel-powered generator? <input type="checkbox"/> yes <input checked="" type="checkbox"/> no
1.9	Are the functionalities in 1.2, 1.3, 1.4, 1.6, 1.7 and 1.8, where present, regularly tested? <input checked="" type="checkbox"/> yes <input type="checkbox"/> no
	<p>In your opinion, are the documented measures appropriate, given the state of the art, implementation costs, nature, scope, context and purposes of the processing as well as the likelihood and severity of the risk for the rights and freedoms of the data subject, such that an appropriate standard of protection is guaranteed?</p> <p><input checked="" type="checkbox"/> Appropriate <input type="checkbox"/> Appropriate with reservations <input type="checkbox"/> Inappropriate</p> <p>Reason:</p>
2	Backup- and emergency concepts, virus protection
2.1	Is a backup concept in place? <input checked="" type="checkbox"/> yes <input type="checkbox"/> no
2.2	Is the functionality of the backup creation regularly tested? <input checked="" type="checkbox"/> yes <input type="checkbox"/> no
2.3	How frequently are backups from systems which store personal data created? <input type="checkbox"/> Real time <input type="checkbox"/> Daily <input type="checkbox"/> One to three times a week

	<input checked="" type="checkbox"/> Other: Please specify Customer data backups are not provided by default and are executed on demand
2.4	On what storage devices are the backups stored? <input checked="" type="checkbox"/> Second redundant server <input type="checkbox"/> Backup Tapes <input type="checkbox"/> Hard drives <input type="checkbox"/> Other: please specify
2.5	Where are the backups stored? <input checked="" type="checkbox"/> Second redundant server at a separate location <input type="checkbox"/> In a safe which is fire resistant and data carrier- and document safe <input type="checkbox"/> in a normal safe <input type="checkbox"/> bank drawer <input type="checkbox"/> lockable drawer / filing cabinet <input type="checkbox"/> in a server room <input type="checkbox"/> private household <input type="checkbox"/> Other: please insert storage location
2.6	Regarding 2.5: Where backups are being transported: how does this occur? <input type="checkbox"/> Taken by an IT employee / Management / Secretary <input type="checkbox"/> Collection by a third party (i.e. bank employee / surveillance company) <input checked="" type="checkbox"/> Other: Please specify By network
2.7	Are the backups encrypted? <input type="checkbox"/> yes <input checked="" type="checkbox"/> no
2.8	Is the backup storage location in a separate fire area from the primary server? <input checked="" type="checkbox"/> yes <input type="checkbox"/> no
2.9	Is there a documented process for software or patch- management? <input checked="" type="checkbox"/> yes <input type="checkbox"/> no <input type="checkbox"/> Process is in place, but is not documented
2.10	If 2.9 yes, who is responsible for the software or patch- management? <input checked="" type="checkbox"/> Administrator themselves <input type="checkbox"/> Internal IT <input type="checkbox"/> External service provider
2.11	Is an emergency concept in place (emergency measures in the event of an emergency, hardware defects, fire, data loss, etc.)? <input checked="" type="checkbox"/> yes <input type="checkbox"/> no
2.12	Are the IT systems technologically protected from data loss / unauthorized data access? Yes, via an always updated <input checked="" type="checkbox"/> Virus protection <input type="checkbox"/> Anti-Spyware <input type="checkbox"/> Spam filter
2.13	If 2.12 yes, who is responsible for the updated virus protection, spyware and spam filter? <input type="checkbox"/> Administrator themselves <input type="checkbox"/> Internal IT <input type="checkbox"/> External service provider
	In your opinion, are the documented measures appropriate, given the state of the art, implementation costs, nature, scope, context and purposes of the processing as well as the likelihood and severity of the risk for the rights and freedoms of the data subject, such that an appropriate standard of protection is guaranteed? <input checked="" type="checkbox"/> Appropriate <input type="checkbox"/> Appropriate with reservations <input type="checkbox"/> Inappropriate Reason:

3	Network connection
3.1	Does the company have a redundant internet connection? <input checked="" type="checkbox"/> yes <input type="checkbox"/> no
3.2	Are the individual locations of the company connected via a redundant connection? <input checked="" type="checkbox"/> yes <input type="checkbox"/> no
3.3	Who is responsible for the network connection of the company? <input checked="" type="checkbox"/> Internal IT <input type="checkbox"/> External service provider
	<p>In your opinion, are the documented measures appropriate, given the state of the art, implementation costs, nature, scope, context and purposes of the processing as well as the likelihood and severity of the risk for the rights and freedoms of the data subject, such that an appropriate standard of protection is guaranteed?</p> <p><input checked="" type="checkbox"/> Appropriate <input type="checkbox"/> Appropriate with reservations <input type="checkbox"/> Inappropriate</p> <p>Reason:</p>