

COMPANY Vendor Assessment Questionnaire - VENDOR

Questions

Section 1: Overall

1. What is the Vendor name?
2. What is the Product name?
3. Please provide a description of the product/tool/service and its purpose
4. What is the main establishment location?
5. What is the data centre location?

Section 2: Privacy

1. What personal data do you process?
2. How do you process personal data?
3. Do you act as a controller, processor or both regarding our data? If both outline for which data/data subjects in each role.
4. Do you have a data protection officer?
5. How do you stay up-to-date with privacy laws?
6. Do you use our data for other purposes? If so, which?

Section 3: Data Centres

1. Who are your hosting partners?
2. Where are the data centres located?
3. What are your security certifications, if any?

Section 4: Data Destruction

1. Describe your policies regarding data destruction
 - a. When data is removed?
 - b. How?
 - c. If we end our business relation, do you destroy/return our data?
2. How do you comply with:
 - a. Right to be forgotten?
 - b. Right to erasure?

Section 5: Data breaches

1. How and when will you notify us of data breaches?
2. Have you experienced a data breach?
3. Do you have a data breach response plan and processes in place?
4. Are you now, or have you been under investigation for any data breaches or breaches of data protection law? If so, please explain the circumstances.

Section 6: Organisational Security

1. Do you have an internal security policy in place?
2. Is there a public document you can share? Or table of contents of your internal policy?
3. How is access and credentials handled?
4. Do you train your staff on security and privacy? If so, how?
5. Is security assessed and monitored continuously?
6. Have you conducted pen tests or other security tests?

7. Do you have security certifications?

Section 7: Technical Security

Logging

1. What kind of logging exists for the access of our data? ‘
2. Do we get access to such logs?
3. How long are logs stored?
4. Are logs encrypted?

Backups

1. How often do you back-up data?
2. How long are backups stored?
3. Are backups encrypted?
4. Do you have an offsite backup location?

Encryption at transfer

1. Are data transfers encrypted?
2. Are intra-application transfers encrypted?

Encryption at rest

1. Is data encrypted at rest?
2. How?

End-point protection

Data segregation

Server infrastructure and patch management?

Access management

Support for Okta / SAML ?

Section 8: Transfer of Data

1. Is data transferred to third parties, such as sub-processors?
If yes:
 - a. Who are they?
 - b. Do data you have data processing agreements in place with these?
 - c. How do you notify us of changes to third parties?
2. Is the data transferred outside EEA or EU adequate regions?
 - a. If yes, where and what safeguards exist

Question Text	Selection	
Here is the question text	xx Selection 1 xx Selection 2 xx Selection 3	
Here is more question text	xx moar se lections xx even morrrr	

End of document.