WORLD ORGANISATION FOR ANIMAL HEALTH
Protecting animals, preserving our future

PROCESSOR ASSESSMENT QUESTIONNAIRE

WORLD ORGANISATION FOR ANIMAL HEALTH

Author	OIE Data Privacy Team
Date	May 19, 2020

CONTENTS

I. DEFINITIONS

- **Personal data** means any information relating to an identified or identifiable natural person (**'data subject'**); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person
- **Processing** means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction
- **Pseudonymisation** means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person
- **Controller** means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data. In this instance, OIE is a controller
- **Processor** means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller
- **Recipient** means a natural or legal person, public authority, agency or another body, to which the personal data are **disclosed**, whether a third party or not
- **Third party** means a natural or legal person, public authority, agency or body **other** than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data
- **Personal data breach** means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed

II. ASSESSMENT SURVEY

Name of the Company:
Address:
Headquarters:
Phone number:
Contact of the DPO (data protection officer) designated to the supervisory authority:
Contact of the CISO:
Author of the survey:
Date:

1. Responsibility

1.1. Have you documented measures to comply with the **General Data Protection Regulation** (GDPR)?

○ Yes

○ No

1.2. With which GDPR requirements are you not in compliance and by which deadline do you expect to be compliant?

……
……
……

1.3. Do you keep a record of processing activities in accordance with article 30 of the GDPR?

○ Yes
○ No

If not, please briefly justify:

……
……
……

1.4. Have you conducted an audit on your data processing operations to assess their compliance to the GDPR?

○ Yes
○ No

If not, please briefly explain why:

……
……
……

2. Implication of third parties

2.1. Do you work with contractors or processors that may have access to OIE's information or personal data processing activities?

○ Yes
○ No

2.2. If the answer is yes, do you have control over their interventions and processing activities on said information and personal data?

○ Yes
○ No

Please briefly detail how:

……
……
……

2.3. Have you made sure that all your processors are providing sufficient guarantees to implement appropriate technical and organisational measures to ensure the confidentiality, integrity, availability, and resilience of the personal data? Can you provide proof of such measures?

○ Yes
○ No

If the answer is yes, please briefly detail:

……
……
……

2.4. Have you signed a contract regarding the processing activities with your processor that meets the requirements of the GDPR?

○ Not yet enforced nor planned
○ Planned but not enforced
○ Partially enforced
○ Successfully enforced with all processors involved

○ N/A
○ I do not know what it is about

2.5. If your processors are located outside the EU or if they process OIE's data outside the EU, what appropriate safeguards are provided to ensure an adequate level of protection?

○ Standard data protection clauses adopted by the European Commission
○ Other standard data protection clauses adopted by a supervisory authority
○ Binding Corporate Rules
○ Privacy Shield
○ Certification: (Detail)…….
○ Other: (Detail)…….

3. Security

3.1. Have you adopted and documented an information systems security policy?

○ Not yet enforced
○ Planned
○ Partially enforced
○ Successfully enforced but not documented
○ Successfully enforced and documented

3.2. Is your security policy adapted to the risks regarding personal data?

○ Yes
○ No
○ I do not know

3.3. Have you implemented encryption measures?

○ Yes: (Detail) ……
○ No

3.4. Do you hold and keep up to date a mapping of IT hardware and software regarding OIE's personal data processing activities?

○ Yes
○ No
○ N/A

Please explain:
……
……
……

3.5. Do you have a complete, registered and up-to-date inventory of high-privilege accounts on the information system of OIE or with access to OIE's personal data and information?

- ○ Yes
- ○ No
- ○ Other: (Detail) ……

3.6. Do you have an arrival and departure management procedure regarding the employees with access to OIE's personal data (staff, interns, etc.)?

- ○ Yes
- ○ No
- ○ Other: (Detail) ……

3.7. Have you implemented an account and rights management policy that follows the "need to know" principle?

- ○ Yes
- ○ No
- ○ Other: (Detail) ……

3.8. Do you forbid the connexion of personal devices on your and OIE's information systems?

- ○ Yes
- ○ No
- ○ Other: (Detail) ……

3.9. Do you keep up to date all of your software's components that may have an impact on OE's processing?

- ○ Yes
- ○ No
- ○ N/A
- ○ Other: (Detail) ……

3.10. Could you briefly describe your authentication management system?

……

……

3.11. Do you comply with good practices for choosing, sizing and renewing passwords?

- ○ Yes
- ○ No
- ○ N/A

Please, detail:

……

……

3.12. Have you implemented technical means to make password rules mandatory?

- ○ Yes
- ○ No
- ○ N/A: (Detail) ……

3.13. Do you keep passwords on computer systems or on paper?

- ○ Yes
- ○ No
- ○ N/A
- ○ Other: (Detail) ……

3.14. Do you systematically delete or change the default authentication elements (passwords, certificates) on equipment (network switches, routers, servers, printers)?

- ○ Yes
- ○ No
- ○ N/A
- ○ Other: (Detail) ……

3.15. Do you implement a homogeneous level of security across your entire information system?

- ○ Yes
- ○ No
- ○ N/A
- ○ Other: (Detail) ……

3.16. Do you technically prohibit the connection of removable devices (e.g., USB flash drives) to your computers that have access to the information system of OIE or that are used to process OIE's personal data?

- ○ Yes
- ○ No
- ○ N/A
- ○ Other: (Detail) ……

3.17. Do you use an asset management tool to deploy security policies and updates on equipment?

- ○ Yes
- ○ No
- ○ N/A
- ○ Other: (Detail) ……

3.18. Do you manage nomadic terminals according to the same security policy as fixed workstations?

- ○ Yes
- ○ No
- ○ N/A
- ○ Other: (Detail) ……

3.19. Do you have measures in place to separate OIE's personal data and information from that of your other customers?

- ○ Yes
- ○ No
- ○ N/A
- ○ Other: (Detail) ……

3.19. Do you prohibit browsing the internet from administration accounts? Do you use a network dedicated to equipment administration or at least a network logically separated from the users' network?

- ○ Yes
- ○ No
- ○ N/A
- ○ Other: (Detail) ……

3.20. Do you use secure interconnection gateways for each Internet access?

- ○ Yes
- ○ No
- ○ N/A

3.21. Do you have a procedure in place for logging connections and events and for analysing logs?

- ○ Yes
- ○ No
- ○ N/A

Please detail:

……
……

3.22. Do you keep proof of the following during identification?

- ○ Date and hour
- ○ User identity
- ○ Accomplished tasks
- ○ None of the above

3.23. Do you systematically use security measures to access the premises?

- ○ Yes
- ○ No
- ○ N/A

Please detail:
……
……

3.24. When dealing with a machine infection, do you try to find out if the malicious code may have spread elsewhere in the network?

- ○ Yes
- ○ No
- ○ N/A

3.25. Do you have a regularly updated IT recovery or business continuity plan?

- ○ Yes
- ○ No
- ○ N/A

Please detail:
……
……

3.26. Do you have detection measures in place and a chain of alerts known to all parties involved to alert OIE without delay in the event of a security breach or a breach of confidentiality of personal data?

- ○ Yes
- ○ Non
- ○ N/A
- ○ Other: (Detail) ……

3.27. Do you regularly raise staff awareness regarding security measures?

- ○ Yes
- ○ No
- ○ N/A
- ○ Other: (Detail) ……

3.28. Do you have periodic security audits carried out? If so, what is the frequency of said audits? Are they all part of an action plan?

- ○ Yes
- ○ No
- ○ N/A
- ○ Other: (Detail)……

4. Anonymisation /pseudonymisation

4.1. Are you able to anonymise OIE's personal data if necessary?

- ○ Yes
- ○ No
- ○ I do not know

4.2. Are you able to implement pseudonymisation measures at OIE's request?

- ○ Yes
- ○ No
- ○ I do not know

5. Servers

5.1. Do your servers store OIE's personal data?

- ○ Yes
- ○ No

Where are they located?

……
……

If your answer is no, please go directly to question 7

5.2. Are your servers accessible via the Internet (no firewall, no DMZ)?

- ○ Yes
- ○ No

5.3. Are they connected to a third party's system of information?

○ Yes
○ No

5.4. Have you implemented a procedure that describes the update of your IT infrastructure (OS, Patch, anti-virus)?

○ Yes
○ No

5.5. In which country are located your backup servers?
……
……

5.6. Are you the owner of those servers?

○ Yes
○ No

5.6.1. If not, Is the owner of the server certified from an IT security perspective on the perimeter regarding personal data and OIE's information (e.g. ISO 27001)?

○ Yes
○ No

5.6.2. In the event of an incident, what are the restoration and remediation measures planned?
……
……

If your information system is hosted by a service provider:

5.6.3. Does this provider provide denial of service protection (DOS/DDOS)?

○ Yes
○ No

5.6.4. Does this service provider ensure the traceability of the operations carried out in your IS (infrastructure logs, database...etc.)?

○ Yes
○ No

5.6.5. Does your provider ensure traceability of the use of privileged accounts and protection of traces against modification?

- ○ Yes
- ○ No

5.6.6. Does this service provider provide protection against malware?

- ○ Yes
- ○ No

5.6.7. Does this service provider have perimeter security measures (Firewall, IDS, IPS, NIDS, HIDS)?

- ○ Yes
- ○ No

5.6.8. Does this service provider ensure the segmentation of the network?

- ○ Yes
- ○ No

5.6.9. Does this service provider have a system for monitoring and detecting security incidents (e.g. SIEM)?

- ○ Yes
- ○ No

5.6.10. Does this service provider provide security patches for components?

- ○ Yes
- ○ No

5.6.11. Does this service provider ensure a regular infrastructure audit?

- ○ Yes
- ○ No

5.6.12. Does this service provider ensure the physical and environmental protection of the datacenters (physical access control, energy, air conditioning, fire, flooding, lightning, earthquake)?

- ○ Yes
- ○ No

5.6.13. Are your provider's datacenters certified?

- ○ Yes
- ○ No

5.6.14. Does your provider provide data encryption (Transit+rest)?

- ○ Yes
- ○ No

5.6.15. Does your provider ensure the deletion of data on storage media in case of hardware scrapping (end of life, failure)?

- ○ Yes
- ○ No

5.6.16. Does your provider have a backup system?

- ○ Yes
- ○ No

5.6.17. Does your provider have a Web application Firewalls (WAF)?

- ○ Yes
- ○ No

5.6.18. Does this service provider ensure the availability of the information system (replication between different datacenters, loadbalancer)?

- ○ Yes
- ○ No

6. Laptops with access to OIE's personal data and information

6.1. Are your employees' laptops protected by a regularly updated anti-virus software?

- ○ Yes
- ○ No

7. Data retention

7.1. Can you manage data retention periods by following OIE's instructions?

- ○ Yes
- ○ No
- ○ In part

If not, please explain why it is not possible as well as the personal data storage period or if not possible, the criteria used to determine that period.

……
……

7.2. At the end of the storage period, how do you manage data erasure?
……
……

8. Individuals with access to OIE's personal data

8.1. Can you ensure that all individuals/contractors with access to personal data are bound by confidentiality obligations?

- ○ Yes
- ○ No

9. Certification

9.1. Have you been issued certifications regarding data protection or security as well as labels? (For example: ISO 27001, CNIL label...)

- ○ Yes
- ○ No

If your answer is yes, please detail.

……

……

10. Data subject's rights management

10.1. Right of access. Have you implemented a process to handle requests by the data subject to access, rectify or erase their personal data, at OIE's request?

- ○ Yes
- ○ No
- ○ I do not know
- ○ N/A

10.2. Does your company frequently, and in a secure manner, delete the personal data of clients' employees (users and admin) by following a data retention management procedure?

- ○ Yes
- ○ No
- ○ I do not know
- ○ N/A

10.3. Right to data portability. Is your company able to convert personal data in a structured, commonly used, and machine-readable format at OIE's request and to transmit those data in a secure manner to any recipient identified by OIE?

- ○ Yes
- ○ No
- ○ I do not know
- ○ N/A

11. IT security policy (ITSP)

Tenderers can attached their ITSP. The submission of the ITSP will be considered an advantage that will be taken into account in the evaluation of tenders.

Date: …… Signature

……

Name and Title of duly authorized representative:

……

……

……

Entity name:

……