PRU/COS2023/1

**Annexe n°3****– QUESTIONNAIRE D’EVALUATION DU TRAITEMENT DES DONNEES PERSONNELLES**

|  |
| --- |
| **ORGANISATION MONDIALE DE LA SANTE ANIMALE (OMSA) DONT LE NOM STATUTAIRE EST “OFFICE INTERNATIONAL DES EPIZOOTIES”** |

# SOMMAIRE

[I. DEFINITIONS 3](#_Toc126678134)

[II. ENQUETE D’EVALUATION 4](#_Toc126678135)

# DEFINITIONS

* **Données à caractère personnel** désigne toute information concernant une personne physique identifiée ou identifiable ("**personne concernée**") ; une personne physique identifiable est une personne qui peut être identifiée, directement ou indirectement, notamment en faisant référence à un identifiant tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne ou à un ou plusieurs éléments spécifiques de l'identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale de cette personne physique.
* **Traitement** désigne toute opération ou ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données ou des ensembles de données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction
* **Pseudonymisation** désigne le traitement de données à caractère personnel effectué de telle sorte que les données à caractère personnel ne puissent plus être attribuées à une personne concernée spécifique sans l'utilisation d'informations supplémentaires, à condition que ces informations supplémentaires soient conservées séparément et fassent l'objet de mesures techniques et organisationnelles visant à garantir que les données à caractère personnel ne sont pas attribuées à une personne physique identifiée ou identifiable.
* **Responsable du traitement** désigne la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement des données à caractère personnel. Dans le cas présent, l’OMSA est un Responsable du traitement de données.
* **Sous-traitant (de traitement des données)** : une personne physique ou morale, une autorité publique, un service ou un autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement des données.
* **Destinataire** désigne une personne physique ou morale, une autorité publique, une agence ou un autre organisme, à qui les données à caractère personnel sont **divulguées**, qu'il s'agisse d'un tiers ou non.
* **Tiers** désigne une personne physique ou morale, une autorité publique, un service ou un organisme **autre** que la personne concernée, le responsable du traitement, le sous-traitant et les personnes qui, sous l'autorité directe du responsable du traitement ou du sous-traitant, sont autorisées à traiter les données à caractère personnel.
* **Violation des données à caractère personnel** désigne une violation de la sécurité entraînant la destruction, la perte, l'altération, la divulgation non autorisée ou l'accès accidentel ou illégal à des données à caractère personnel transmises, stockées ou traitées de toute autre manière.

# ENQUETE D’EVALUATION

Nom de l’entreprise :

Adresse :

Siège :

Numéro de téléphone :

Contact du DPO (*data protection officer*) désigné auprès de l'autorité de contrôle :

Contact du CISO:

Auteur de l’enquête :

Date :

1. **Responsabilité**
   1. Avez-vous répertorié les mesures prises pour vous conformer au **Règlement Général sur la Protection des Données** (RGPD) ?

Oui

Non

* 1. Quelles sont les exigences du RGPD avec lesquelles vous n'êtes pas en conformité et à quelle date pensez-vous être en conformité ?

………………………………………………………………………………………………………………………………………………………………………….……………………………………………………………………………………………………………………………………………………………….……………………………………………………………………………………………………………………………………………………

* 1. Conservez-vous un registre des activités de traitement conformément à l'article 30 du RGPD?

Oui

Non

Si non, merci de préciser brièvement pourquoi :

………………………………………………………………………………………………………………………………………………………………………….……………………………………………………………………………………………………………………………………………………………….……………………………………………………………………………………………………………………………………………………

* 1. Avez-vous réalisé un audit sur vos opérations de traitement des données pour évaluer leur conformité au RGPD ?

Oui

Non

Si non, merci de préciser brièvement pourquoi :

………….……………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………….……………………………………………………………………………………………………………………………………………………

1. **Implication de tiers**
   1. Travaillez-vous avec des prestataires ou des sous-traitants qui peuvent avoir accès aux informations ou aux activités de traitement des données personnelles de l’OMSA ?

Oui

Non

* 1. Si la réponse est oui, exercez-vous un contrôle sur leurs interventions et leurs activités de traitement sur lesdites informations et données personnelles ?

Oui

Non

Merci de préciser brièvement comment :

………….……………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………….…………………………………………………………………………………………………………

* 1. Vous êtes-vous assuré que tous vos sous-traitants fournissent des garanties suffisantes pour mettre en œuvre des mesures techniques et organisationnelles appropriées pour assurer la confidentialité, l'intégrité, la disponibilité et la résilience des données personnelles ? Pouvez-vous apporter la preuve de ces mesures ?

Oui

Non

Si oui, merci de détailler brièvement :

………………………………………………………………………………………………………………………………………………………………………….……………………………………………………………………………………………………………………………………………………………….……………………………………………………………………………………………………………………………………………………

* 1. Avez-vous signé un contrat concernant les activités de traitement avec votre sous-traitant qui répond aux obligations du RGPD ?

Pas encore appliqué ou prévu

Prévu mais pas appliqué

Partiellement appliqué

Appliqué avec succès par tous les sous-traitants

N/A

Je ne sais pas de quoi il s'agit

* 1. Si vos sous-traitants sont situés en dehors de l'UE ou s'ils traitent les données de l’OMSA en dehors de l'UE, quelles garanties appropriées sont fournies pour assurer un niveau de protection adéquat ?

Clauses types de protection des données adoptées par la Commission Européenne

Autres clauses types de protection des données adoptées par une autorité de contrôle

Règles d'entreprise contraignantes

Bouclier de protection des données

Certification : (préciser)………….

Autre : (préciser)………….

1. **Sécurité**
   1. Avez-vous adopté et rédigé une politique de sécurité des systèmes d'information (PSSI)?

Pas encore appliquée

Prévue

Partiellement appliquée

Appliquée avec succès mais pas rédigée

Appliquée avec succès et rédigée

Les soumissionnaires devront joindre leur PSSI.

* 1. Votre politique de sécurité est-elle adaptée aux risques concernant les données personnelles ?

Oui

Non

Je ne sais pas

* 1. Avez-vous mis en place des mesures de cryptage ?

Oui : (préciser) ……………………………………………………………………………

Non

* 1. Disposez-vous et maintenez-vous à jour une cartographie du matériel et des logiciels informatiques concernant les activités de traitement des données personnelles de l’OMSA ?

Oui

Non

N/A

Merci de préciser :   
………………………………………………………………………………………………………………………………………………………………………….……………………………………………………………………………………………………………………………………………………………

* 1. Disposez-vous d'un inventaire complet, répertorié et à jour des comptes à haut privilège sur le système d'information de l’OMSA ou ayant accès aux données et informations personnelles de l’OMSA ?

Oui

Non

Autre : (préciser) ………………………………………………………………………

* 1. Disposez-vous d'une procédure de gestion des arrivées et des départs des employés ayant accès aux données personnelles de l’OMSA (personnel, stagiaires, etc.) ?

Oui

Non

Autre : (préciser) …………………………………………………………………………

* 1. Avez-vous mis en place une politique de gestion des comptes et des droits qui respecte le principe du "besoin de savoir" (“accès sélectif”) ?

Oui

Non

Autre : (préciser) ………………………………………………………………………

* 1. Interdisez-vous la connexion d'appareils personnels sur vos systèmes d'information et ceux de l’OMSA ?

Oui

Non

Autre : (préciser) ………………………………………………………………………

* 1. Actualisez-vous tous les composants de vos logiciels susceptibles d'avoir un impact sur le traitement de l’environnement opérationnel ?

Oui

Non

N/A

Autre : (préciser) ……………………………………………………………………

* 1. Pouvez-vous décrire brièvement votre système de gestion de l'authentification ?

………………………………………………………………………………………………………………………………………………………………………….………………………………………………

* 1. Respectez-vous les bonnes pratiques en matière de choix, de taille et de renouvellement des mots de passe ?

Oui

Non

N/A

Veuillez préciser :

………………………………………………………………………………………………………………………………………………………………………….……………………………………………………………………………………………………………………………………………………

* 1. Avez-vous mis en œuvre des moyens techniques pour rendre obligatoires les règles relatives aux mots de passe ?

Oui

Non

N/A: (préciser) ………………………………………………………………………

* 1. Conservez-vous les mots de passe sous forme électronique ou sur papier ?

Oui

Non

N/A

Autre : (préciser) ………………………………………………………………………

* 1. Supprimez-vous ou modifiez-vous systématiquement les éléments d'authentification par défaut (mots de passe, certificats) des équipements (commutateurs réseau, routeurs, serveurs, imprimantes, etc.) ?

Oui

Non

N/A

Autre : (préciser) ………………………………………………………………………

* 1. Mettez-vous en œuvre un niveau de sécurité homogène sur l'ensemble de vos systèmes d'information ?

Oui

Non

N/A

Autre : (préciser) ……………………………………………………………………

* 1. Interdisez-vous techniquement la connexion de dispositifs amovibles (par exemple, des clés USB) à vos ordinateurs qui ont accès au système d'information de l’OMSA ou qui sont utilisés pour traiter les données personnelles de l’OMSA ?

Oui

Non

N/A

Autre : (préciser) ……………………………………………………………………

* 1. Utilisez-vous un outil de gestion des actifs pour mettre en œuvre les politiques de sécurité et les mises à jour sur les équipements ?

Oui

Non

N/A

Autre : (préciser) ……………………………………………………………………

* 1. Gérez-vous vos postes nomades selon la même politique de sécurité que les postes de travail fixes ?

Oui

Non

N/A

Autre : (préciser) ……………………………………………………………………

3.19. Existe-t-il des mesures pour séparer les données et informations personnelles de l’OMSA de celles de vos autres clients ?

Oui

Non

N/A

Autre : (préciser) ……………………………………………………………………

* 1. Interdisez-vous la navigation sur Internet à partir des comptes administrateurs ? Utilisez-vous un réseau dédié à l'administration des équipements ou au moins un réseau logiquement séparé du réseau des utilisateurs ?

Oui

Non

N/A

Autre : (préciser) ……………………………………………………………………

* 1. Utilisez-vous des passerelles d'interconnexion sécurisées pour chaque accès Internet?

Oui

Non

N/A

* 1. Avez-vous mis en place une procédure d'enregistrement des connexions et des événements et d'analyse des journaux d’exploitation?

Oui

Non

N/A

Merci de préciser :

…………………………………………………………………………………………………………..……………………………………………………………………………………………

* 1. Conservez-vous les preuves des éléments suivants lors de l'identification ?

Date et heure

Identité de l’utilisateur

Tâches effectuées

Aucun

* 1. Utilisez-vous systématiquement des mesures de sécurité pour accéder aux locaux ?

Oui

Non

N/A

Merci de préciser :

…………………………………………………………………………………………………………..……………………………………………………………………………………………

* 1. En cas d'infection d'une machine par un virus, essayez-vous de savoir si le code malveillant a pu se propager ailleurs dans le réseau ?

Oui

Non

N/A

* 1. Disposez-vous d'un plan de reprise d’activité (PRA) ou de continuité de service (PCS) régulièrement mis à jour ?

Oui

Non

N/A

Merci de préciser :

…………………………………………………………………………………………………………..……………………………………………………………………………………………

* 1. Disposez-vous de mesures de détection en vigueur et d'une chaîne d'alerte connue de toutes les parties concernées pour alerter sans délai l’OMSA en cas de violation de la sécurité ou de la confidentialité des données personnelles ?

Oui

Non

N/A

Autre : (préciser) ……………………………………………………………………

* 1. Sensibilisez-vous régulièrement le personnel aux mesures de sécurité ?

Oui

Non

N/A

Autre : (préciser) ……………………………………………………………………

* 1. Faites-vous réaliser des audits de sécurité réguliers ? Si oui, quelle est la fréquence de ces audits ? Font-ils tous partie d'un plan d'action ?

Oui

Non

N/A

Autre : (préciser) ……………………………………………………………………

1. **Anonymisation /pseudonymisation** 
   1. Êtes-vous en mesure d'anonymiser les données personnelles de l’OMSA si nécessaire?

Oui

Non

Je ne sais pas

* 1. Êtes-vous en mesure de mettre en œuvre des mesures de pseudonymisation sur demande de l’OMSA ?

Oui

Non

Je ne sais pas

1. **Serveurs** 
   1. Vos serveurs stockent-ils les données personnelles de l’OMSA ?

Oui

Non

Où sont-ils situés ?

…………………………………………………………………………………………………………..……………………………………………………………………………………………

**Si votre réponse est non, veuillez passer directement à la question 7**

* 1. Vos serveurs sont-ils accessibles via Internet (sans pare-feu, sans DMZ) ?

Oui

Non

* 1. Sont-ils connectés au système d'information d'un tiers ?

Oui

Non

* 1. Avez-vous mis en place une procédure décrivant la mise à jour de votre infrastructure informatique (OS, Patch, anti-virus) ?

Oui

Non

* 1. Dans quel pays sont situés vos serveurs de sauvegarde ?

…………………………………………………………………………………………………………………………………………………………………………………………………………

* 1. Êtes-vous le propriétaire de ces serveurs ?

Oui

Non

* + 1. Si non, le propriétaire du serveur est-il certifié du point de vue de la sécurité informatique sur le périmètre concernant les données personnelles et les informations de l’OMSA (par exemple ISO 27001) ?

Oui

Non

* + 1. En cas d'incident, quelles sont les mesures de restauration et de correction prévues ? …………………………………………………………………………………………………………………………………………………………………………………………………………

**Si votre système d'information est hébergé par un prestataire de services :**

* + 1. Ce prestataire offre-t-il une protection contre le déni de service (DOS/DDOS) ?

Oui

Non

* + 1. Ce prestataire assure-t-il la traçabilité des opérations effectuées dans votre SI (journaux d'infrastructure, base de données...etc.) ?

Oui

Non

* + 1. Votre prestataire assure-t-il la traçabilité de l'utilisation des comptes à privilèges et la protection des traces contre la modification ?

Oui

Non

* + 1. Ce prestataire de services offre-t-il une protection contre les logiciels malveillants ?

Oui

Non

* + 1. Ce prestataire de services dispose-t-il de mesures de sécurité périmétriques (pare-feu, IDS, IPS, NIDS, HIDS) ?

Oui

Non

* + 1. Ce prestataire de services assure-t-il la segmentation du réseau ?

Oui

Non

* + 1. Ce prestataire de services dispose-t-il d'un système de surveillance et de détection des incidents de sécurité (tel que SIEM) ?

Oui

Non

* + 1. Ce prestataire de services fournit-il des correctifs de sécurité pour les composants ?

Oui

Non

* + 1. Ce prestataire de services assure-t-il un audit régulier de l'infrastructure ?

Oui

Non

* + 1. Ce prestataire de services assure-t-il la protection physique et environnementale des centres de données (contrôle d'accès physique, énergie, climatisation, incendie, inondation, foudre, tremblement de terre) ?

Oui

Non

* + 1. Les centres de données de votre prestataire sont-ils certifiés ?

Oui

Non

* + 1. Votre prestataire assure-t-il le cryptage des données (Transit+rest) ?

Oui

Non

* + 1. Votre prestataire assure-t-il la suppression des données sur les supports de stockage en cas de mise au rebut du matériel (fin de vie, panne) ?

Oui

Non

* + 1. Votre prestataire dispose-t-il d'un système de sauvegarde ?

Oui

Non

* + 1. Votre fournisseur dispose-t-il d'un pare-feu pour les applications Web (WAF) ?

Oui

Non

* + 1. Ce prestataire assure-t-il la disponibilité du système d'information (réplication entre différents centres de données, répartiteurs de charge) ?

Oui

Non

1. **Ordinateurs portables ayant accès aux données et informations personnelles de l’OMSA**
   1. Les ordinateurs portables de vos employés sont-ils protégés par un logiciel anti-virus régulièrement mis à jour ?

Oui

Non

1. **Conservation des données**

* 1. Pouvez-vous gérer les périodes de conservation des données en suivant les instructions de l’OMSA ?

Oui

Non

Partiellement

Si ce n'est pas le cas, veuillez en indiquer les raisons ainsi que la durée de conservation des données personnelles ou, si ce n'est pas possible, les critères utilisés pour déterminer cette durée.

………………………………………………………………………………………………………….…………………………………………………………………………………………

* 1. A la fin de la période de stockage, comment gérez-vous l'effacement des données ?

………………………………………………………………………………………………………….……………………………………………………………………………………………..

1. **Personnes ayant accès aux données personnelles de l’OMSA**
   1. Pouvez-vous garantir que tous les individus/prestataires ayant accès aux données personnelles sont liés par des obligations de confidentialité ?

Oui

Non

1. **Certification** 
   1. Avez-vous obtenu des certifications concernant la protection ou la sécurité des données ainsi que des labels ? (Par exemple : ISO 27001, label CNIL...)

Oui

Non

Si votre réponse est oui, veuillez préciser.……………………………….……………………

………………………………………………………………………………………………………………………………………………….

1. **Gestion des droits de la personne concernée**
   1. Droit d'accès. Avez-vous mis en place un processus pour traiter les demandes d'accès, de rectification ou d'effacement des données personnelles de la personne concernée, à la demande de l’OMSA ?

Oui

Non

Je ne sais pas

N/A

* 1. Votre entreprise supprime-t-elle fréquemment, et de manière sécurisée, les données personnelles des employés des clients (utilisateurs et administrateurs) en suivant une procédure de gestion de la conservation des données ?

Oui

Non

Je ne sais pas

N/A

* 1. Droit à la portabilité des données. Votre entreprise est-elle en mesure de convertir les données personnelles dans un format structuré, couramment utilisé et lisible en format informatique sur demande de l’OMSA et de transmettre ces données de manière sécurisée à tout destinataire identifié par l’OMSA ?

Oui

Non

Je ne sais pas

N/A

Date : …………………………….

Signature ………………………………………………………….

Nom et fonction du représentant dûment habilité :……………………………………………

Nom de l’entité :……………………………………………………………………………………..