BTS SIO · BLOC 3 CYBERSÉCURITÉ

Audit MedSecure — Recensement des DCP et conformité RGPD

Nom :	Note :
.....	..... / 20

Durée conseillée : 1 h 30 · Évaluation sur 20 points

Consigne : Répondez de manière rédigée et justifiez vos choix à partir du dossier documentaire de l'audit. Utilisez le vocabulaire précis des fiches savoir.

Mission 1 — Recensement, typologie des données et minimisation · 10 points

1. **Rappelez précisément ce qui caractérise une donnée à caractère personnel (DCP) et une donnée sensible selon l'article 9 du RGPD.** — **3 pts**

2. **À partir des tables du document 1 :** — **4 pts**

- **a) dans la table `Patient`, relevez deux DCP simples (directes ou indirectes) ;**
- **b) relevez une donnée sensible et justifiez pourquoi elle l'est selon le RGPD ;**
- **c) indiquez si les informations de la table `CabinetMedical` sont des DCP et justifiez précisément votre réponse.**

3. **Dans le formulaire d'inscription du document 2, identifiez les deux renseignements qui contreviennent clairement au principe de minimisation. Justifiez pourquoi leur collecte est illégale et indiquez la mesure corrective attendue.** — **3 pts**

Mission 2 — Registres RGPD et traitement d’une violation de données · 10 points

4. **Nommez le document obligatoire prévu par l’article 30 du RGPD dans lequel MedSecure consigne ses activités de traitement, leurs finalités et leurs durées de conservation.** **2 pts**

5. **À partir du ticket d’incident critique (document 3) et du guide CNIL (document 4) :** **4 pts**

- **a) indiquez si l’exfiltration constitue une violation de données personnelles au sens du RGPD et justifiez ;**
- **b) nommez l’autorité administrative à notifier et calculez la date et l’heure limites exactes de notification à partir de la date de confirmation (14/04/2025 à 09 h 15).**

6. **À partir du ticket d’incident (document 3) et des règles légales :** **4 pts**

- **a) les 4 200 patients doivent-ils être individuellement informés ? Justifiez en fonction de la nature des données dérobées et du niveau de risque pour leurs droits et libertés ;**
- **b) nommez le registre interne obligatoire prévu par l’article 33.5 du RGPD où MedSecure doit consigner cet incident (même en l’absence de notification CNIL) et citez deux éléments qui doivent y figurer.**