Check-list avis DPO

1. Situation et contexte

(→ par le DPO et le responsable du traitement/sous-traitant)

- ***Législation et réglementation applicable***
- ***Organisation***
- ***Description du traitement***

2. Analyse et avis

(→ par le DPO ; une bonne pratique consiste à également mentionner quand un principe ou un droit déterminé ne s'applique pas, démontrant ainsi qu'une évaluation a été effectuée et profitant à l'obligation de documentation)

- ***Licéité et loyauté (RGPD, art. 5.1.a)***
  - En cas d'intérêt légitime : 'balance test' (test de pondération) et argumentation inclus ;
  - En cas d'obligation légale : renvoi à la législation applicable ;
  - En cas d'intérêt public ; renvoi à la mission dans la législation applicable pour laquelle le traitement est nécessaire ;
  - En cas de consentement : évaluation/avis concernant les conditions du consentement, ex. droit de retrait du consentement
- ***Limitation des finalités (RGPD, art. 5.1.b)***
- ***Minimisation des données (RGPD, art. 5.1.c)***
- ***Exactitude (RGPD, art. 5.1.d)***
- ***Limitation de la conservation (RGPD, art. 5.1.e)***
- ***Analyse du (des) traitement(s) (e.a. RGPD, art. 24.1 et art. 39.2)***
  - Catégories de données à caractère personnel
    (Ex. numéro de Registre national/numéro national, catégories particulières de données à caractère personnel, coordonnées, données financières, ...)
  - Catégories de personnes concernées
    (Ex. en interne (ex. des collaborateurs), en externe (ex. des clients))
  - Décision individuelle automatisée, y compris le profilage
  - Autres aspects concernant la nature, la portée et le contexte du traitement
- ***Protection des données dès la conception et protection des données par défaut (RGPD, art. 25)***
- ***Gestions des risques et Analyse d'impact relative à la protection des données (e.a. RGPD, art. 24 et 35)***
  (Ex. Analyse révélant qu'une Analyse d'impact relative à la protection des données est nécessaire ou non ; le résultat de l'Analyse d'impact relative à la protection des données, on peut éventuellement faire un renvoi ici à la politique de sécurité de l'information ou à une autre documentation à ce sujet, ...)
- ***Sécurité du traitement (e.a. RGPD, art. 32 et art. 24.1-2)***
  (Ici aussi, on peut éventuellement faire un renvoi à la politique de sécurité de l'information ou à une autre documentation à ce sujet.)

- Mesures en matière de confidentialité, d'intégrité et de disponibilité ;
- Mesures en matière de relations externes (tant au sein qu'en dehors de l'EEE) et de responsabilité (ex. contrat de sous-traitance, accord entre responsables conjoints du traitement, ...);
- Autres mesures (ex. code de conduite, certification, ...)
- Gestion des fuites de données, y compris notification à l'autorité de contrôle et éventuellement communication à la (aux) personne(s) concernée(s)

- ***Droits des personnes concernées (RGPD, art. 12-23)***
  (Pour chaque droit, il peut être recommandé d'évaluer d'une part s'il est applicable et d'autre part la manière dont l'exercice de ce droit est facilité)

  - Transparence et obligation d'information (RGPD, art. 4.1.a et art. 12-14)
  - Droit d'accès et droit d'obtenir une copie (RGPD, art. 15)
  - Droit de modification ou de rectification (RGPD, art. 16)
  - Droit à l'effacement ou droit à l'oubli (RGPD, art. 17)
  - Droit à la limitation du traitement (RGPD, art. 18)
  - Obligation de notification au destinataire en cas de rectification, effacement et/ou limitation du traitement (RGPD, art. 19)
  - Droit à la portabilité des données (RGPD, art. 20)
  - Droit d'opposition (RGPD, art. 21)
  - Droit de ne pas faire l'objet d'une décision individuelle automatisée (RGPD, art. 22)
  - Droit de retirer son consentement (RGPD, art. 7.3)
  - *Limitations (RGPD, art. 23)*

3. Décision

(→ par le responsable du traitement/le sous-traitant)

4. Exécution

(→ par le responsable du traitement/le sous-traitant)

5. Évaluation

(→ par le DPO)