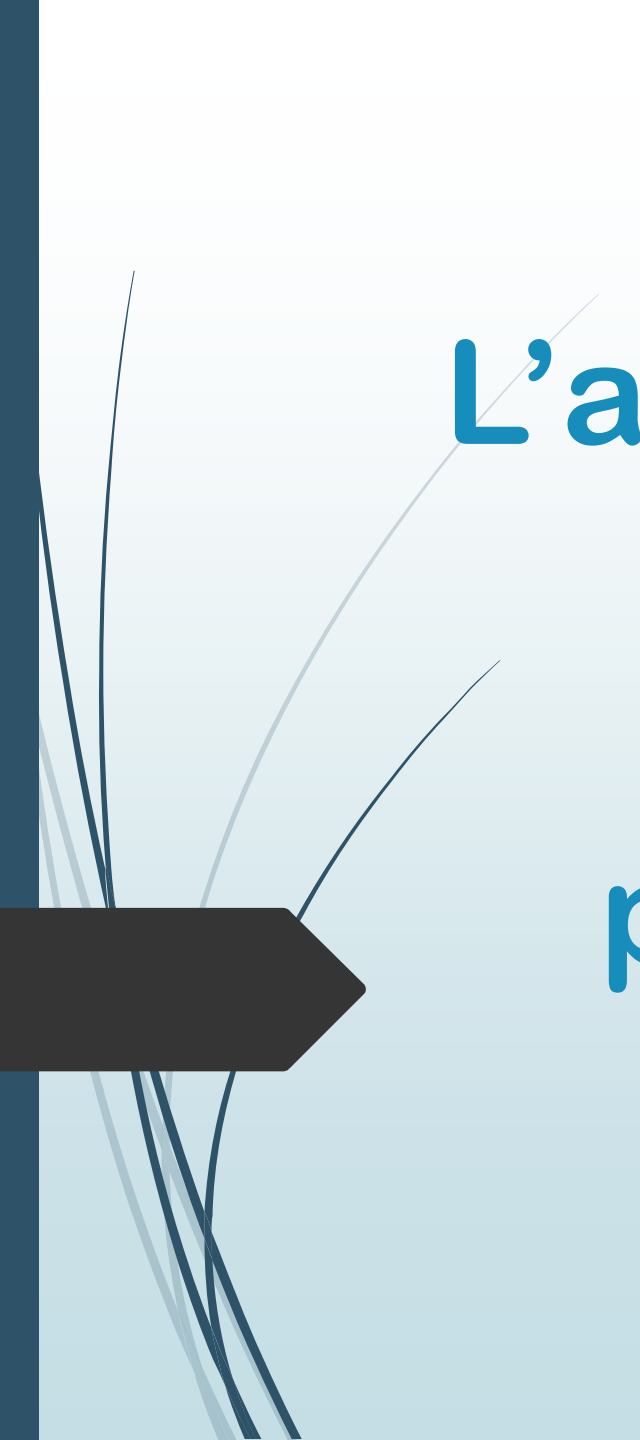




L'analyse d'Impacte relative à la Protection des Données(AIPD) par étapes successives

Sorin Lazarescu – Plateforme DPD – UCVW - 9 nov. 2021

Statistiques

DPO – **34 fois**

Risque(s) – **78 fois**

Protection – **306 fois**

1. Définitions

Ne pas confondre « **risque** » et « **danger** » !

Le risque associe une idée d'incertitude au danger

1. Définitions

Événement:

Occurrence ou changement d'un ensemble particulier de circonstances

1. Définitions

Le risque: (ISO 73:2009)

Probabilité

qu'un événement ou une menace déterminé(e) se produise...

Gravité

..., entraînant un impact déterminé

1. Définitions

Dans notre cas, on traite les risques pour les droits et libertés des personnes physiques

1. Définitions

... un "**risque**" est donc une possibilité qu'une conséquence négative pour les droits et libertés des personnes physiques survienne, suite à un traitement de données à caractère personnel.

2. AIPD

Une AIPD n'est requise que lorsque le traitement de données est susceptible d'engendrer un

risque élevé

pour les droits et libertés des personnes physiques.

(Art. 35.1 RGPD)

2. AIPD

Loi du 30.07.2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel – Loi organique

Une analyse d'impact spécifique de protection des données est effectuée avant l'activité de traitement, même si une analyse d'impact générale relative à la protection des données a déjà été réalisée dans le cadre de l'adoption de la base légale

3. Risque élevé

Qu'est-ce qu'un "risque élevé" ?

Pas de définition dans le RGPD!

3. Risque élevé

L'AIPD est requise particulièrement dans les cas suivants (Art. 35.3 RGPD):

- a) traitement automatisé, y compris le profilage
- b) traitement à grande échelle de données sensibles
- c) la surveillance systématique à grande échelle d'une zone accessible au public

3. Risque élevé

Les données sensibles susceptibles de révéler détails de la sphère intime d'une personne (Art. 9,1 RGPD) :

- origine raciale ou ethnique
- opinions politiques
- convictions religieuses ou philosophiques
- appartenance syndicale
- données génétiques
- données biométriques aux fins d'identifier une personne physique de manière unique
- données concernant la santé
- données concernant la vie sexuelle ou l'orientation sexuelle
- passé judiciaire

3. Risque élevé

Liste des traitements nécessitant une AIPD publiée par l'APD (cf. Art.35.4 RGPD)

1. données biométriques
2. données qui peuvent être utilisées dans une décision de refuser ou de cesser un contrat
3. données de santé collectées par voie automatisée à l'aide d'un dispositif médical implantable actif

3. Risque élevé

Liste APD, suite

4. données collectées à grande échelle afin d'analyser ou de prédire la situation économique, la santé, les préférences ou centres d'intérêt personnels, la fiabilité ou le comportement, la localisation ou les déplacements de personnes physiques
5. des données de nature très personnelle (comme des données sur la pauvreté, le chômage, l'implication de l'aide à la jeunesse ou le travail social, des données sur les activités domestiques et privées, des données de localisation)
6. données générées au moyen d'appareils connectés dotés de capteurs qui envoient des données via Internet ou via un autre moyen (l'Internet des objets)

3. Risque élevé

Liste APD, suite

7. données de communication, de métadonnées ou de données de localisation de personnes physiques ou permettant de mener à des personnes physiques (par exemple le wifi-tracking ou le traitement de données de localisation de voyageurs dans les transports publics) lorsque le traitement n'est pas strictement nécessaire
8. données utilisées dans des applications innovantes
9. données à caractère personnel à grande échelle où le comportement de personnes physiques est observé, collecté, établi ou influencé, y compris à des fins publicitaires, et ce de manière systématique via un traitement automatisé

3. Risque élevé - exceptions

Aucune APID n'est requise:

Le traitement se trouve dans la liste des types d'opérations de traitement publiée par l'APD (Art 35.5 RGPD)

1. obligation légale
2. administration des salaires
3. administration du personnel
4. comptabilité
5. administration des actionnaires et associés
6. fondation, association ou toute autre institution sans but lucratif
7. enregistrement de visiteurs dans le cadre d'un contrôle d'accès

3. Risque élevé - exceptions

Aucune APID n'est requise (suite):

Lorsque le traitement est nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique a une base juridique dans le droit de l'Union ou dans le droit de l'État membre auquel le responsable du traitement est soumis (Art. 35.10 RGPD)

3. Risque élevé

Voir aussi la liste de la CNIL

- données transférées en dehors de l'UE

4. AIPD - décision

Si un traitement répond à deux critères,
une AIPD doit être réalisée !

Plus le nombre de critères auxquels le traitement
répond est élevé, plus il est probable qu'il implique un risque élevé

4. AIPD – les étapes

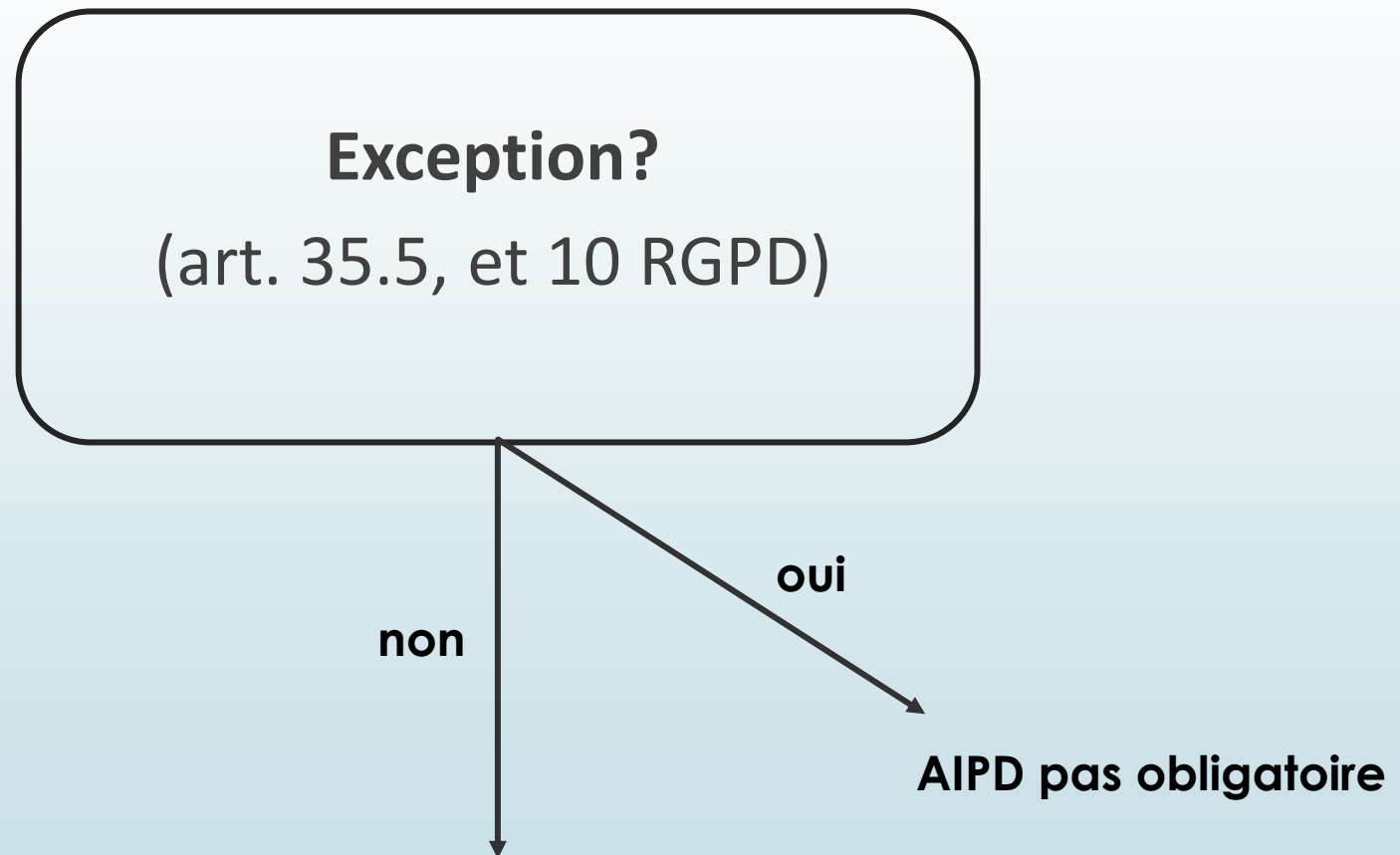
**Le traitement envisagé,
est-il susceptible d'engendrer
des risques élevés?**
(art. 35.1, 3 et 4)

oui

non

AIPD pas obligatoire

4. AIPD – les étapes



4. AIPD – méthodologie

Démontrer :

- respect des principes et droits fondamentaux fixés par le RGPD
- les risques sont maîtrisés via des mesures de sécurité

4. AIPD – méthodologie

Appréciation des risques à la vie privée liés aux données

(Risque = 1 événement redouté + n x menaces permettant que l'événement survienne)

4. AIPD – méthodologie

Type d'évènement redouté

- accès illégitime
- altération non désirée des données
- disparition des données

4. AIPD – méthodologie

Pour chaque évènement redouté, déterminer :

- impacts potentiels sur la vie privée (sentiments d'attentes à la vie privée)

- estimer la gravité des risques

(Faible : 1 ; Moyenne : 2 ; Grave : 3 ; Très grave : 4)

- estimer la vraisemblance des risques

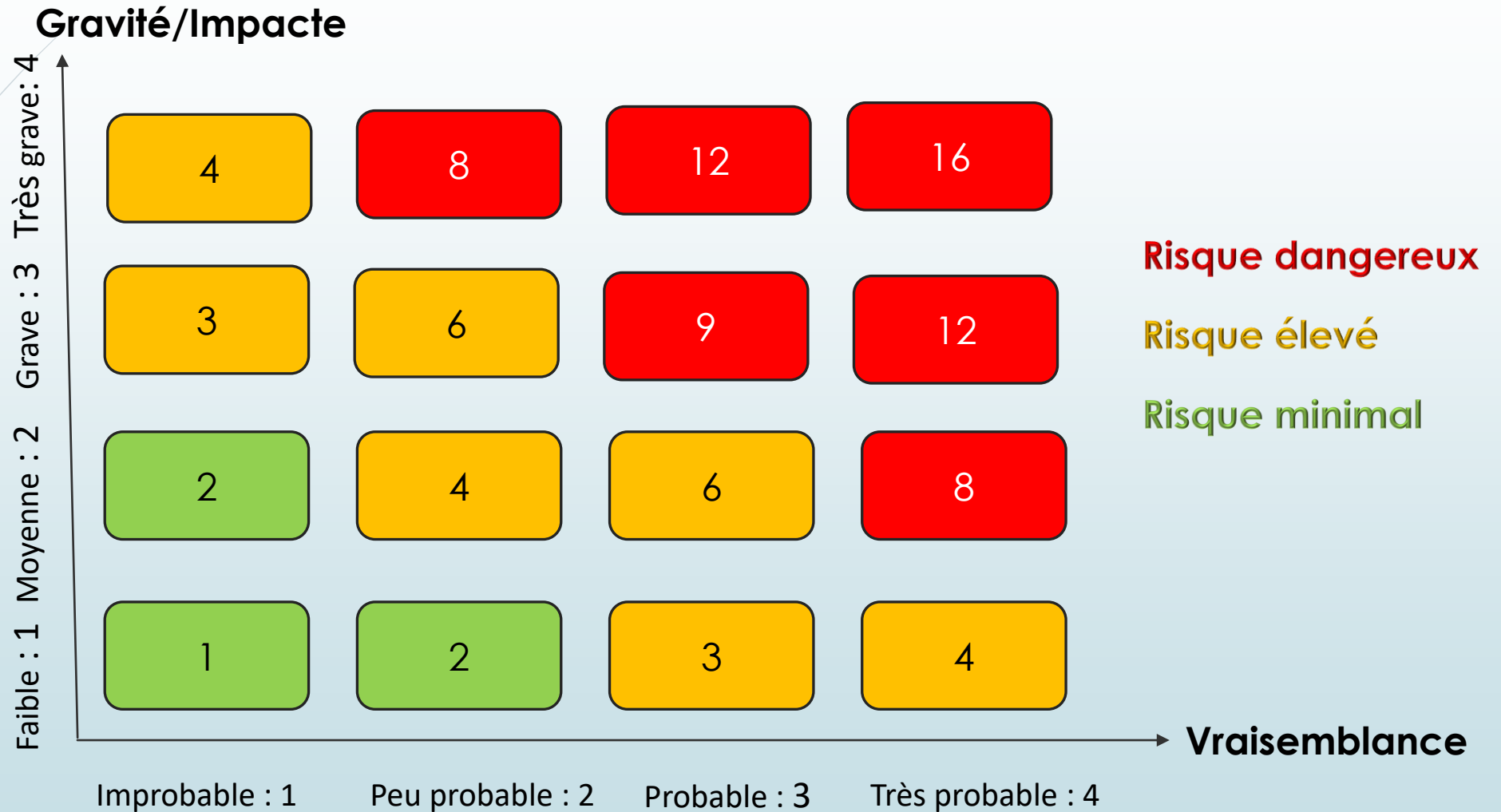
(Improbable : 1 ; Peu probable (rare) : 2 ; Probable (possible) : 3 ; Très probable (Fréquente) : 4)

4. AIPD – méthodologie

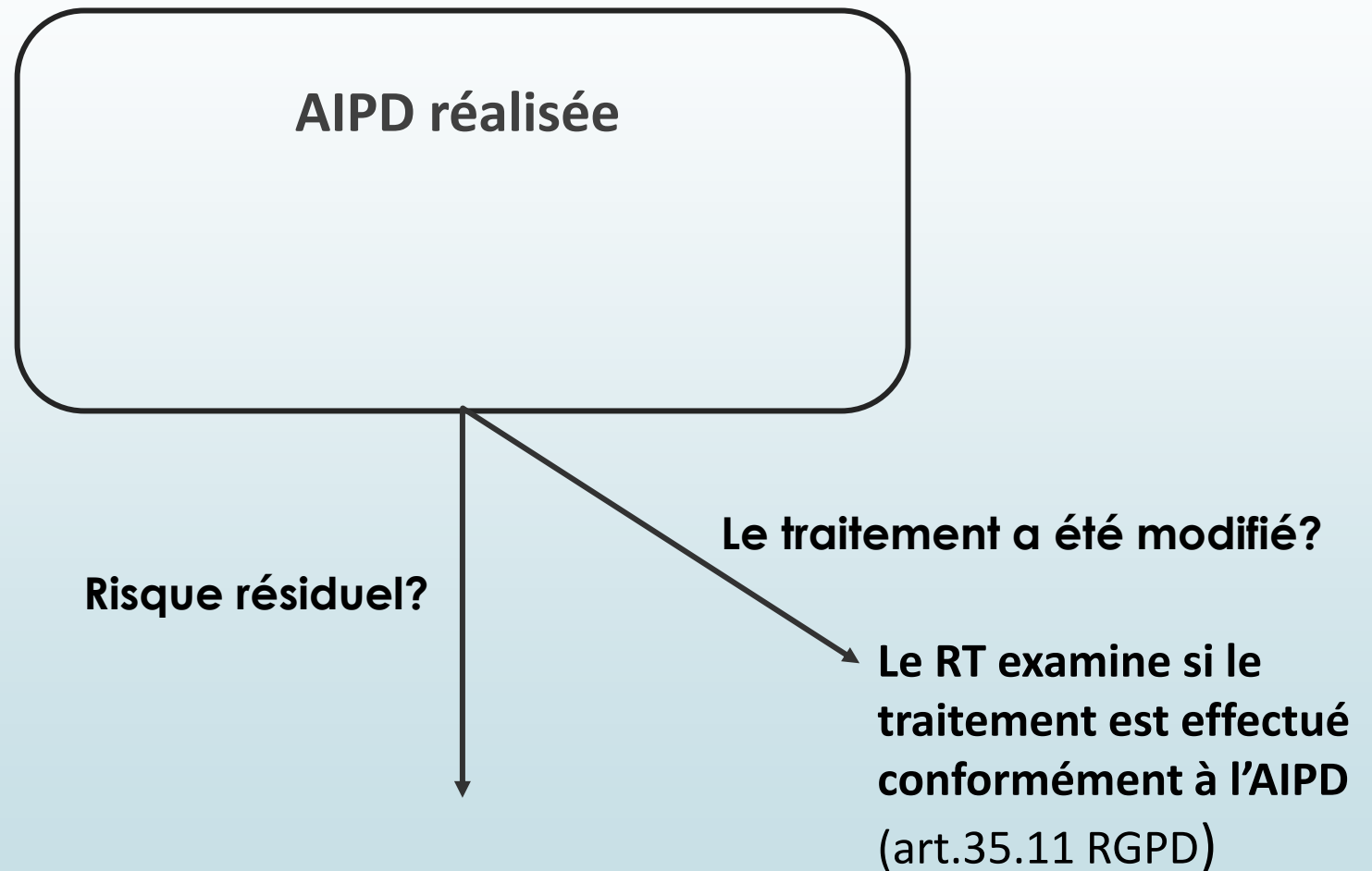
Matrice des risques

Criticité = Gravité x Vraisemblance

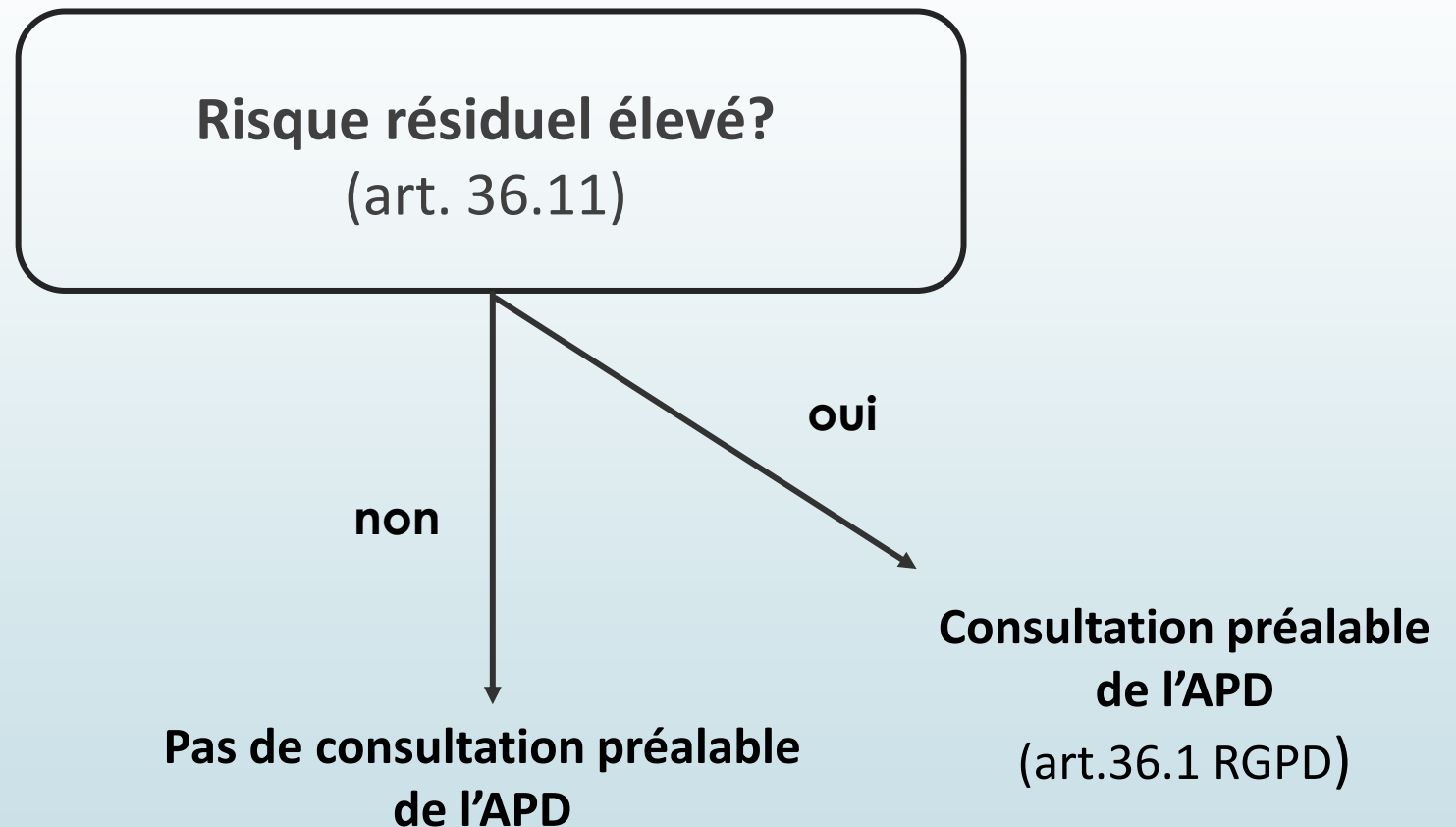
4. AIPD – méthodologie



4. AIPD – les étapes



4. AIPD – les étapes



Sorin LAZARESCU

@ dpd@dpd12.be

☎ 0495 – 321 369

