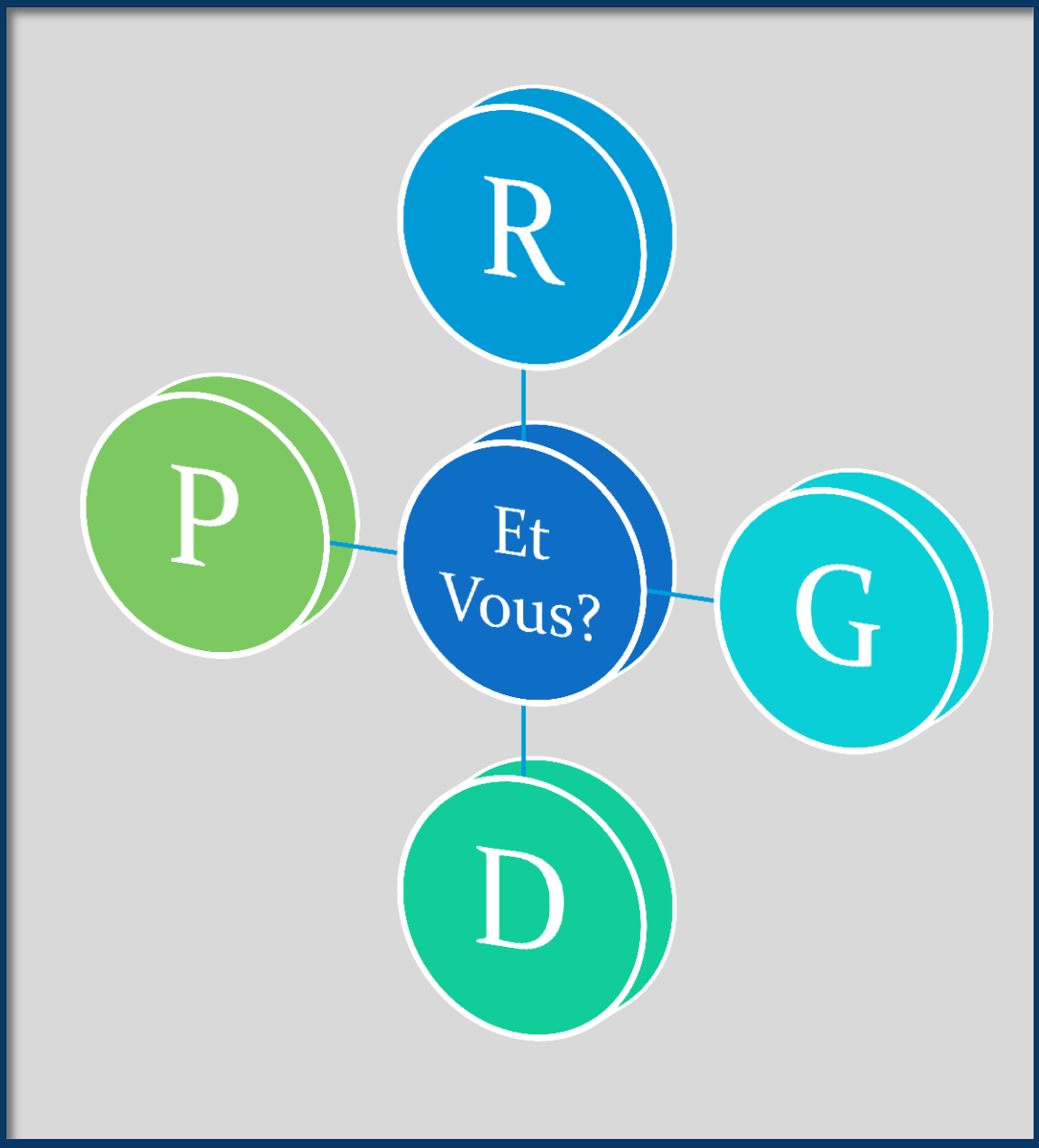

R
P
Et
Vous?
G
D

SOMMAIRE

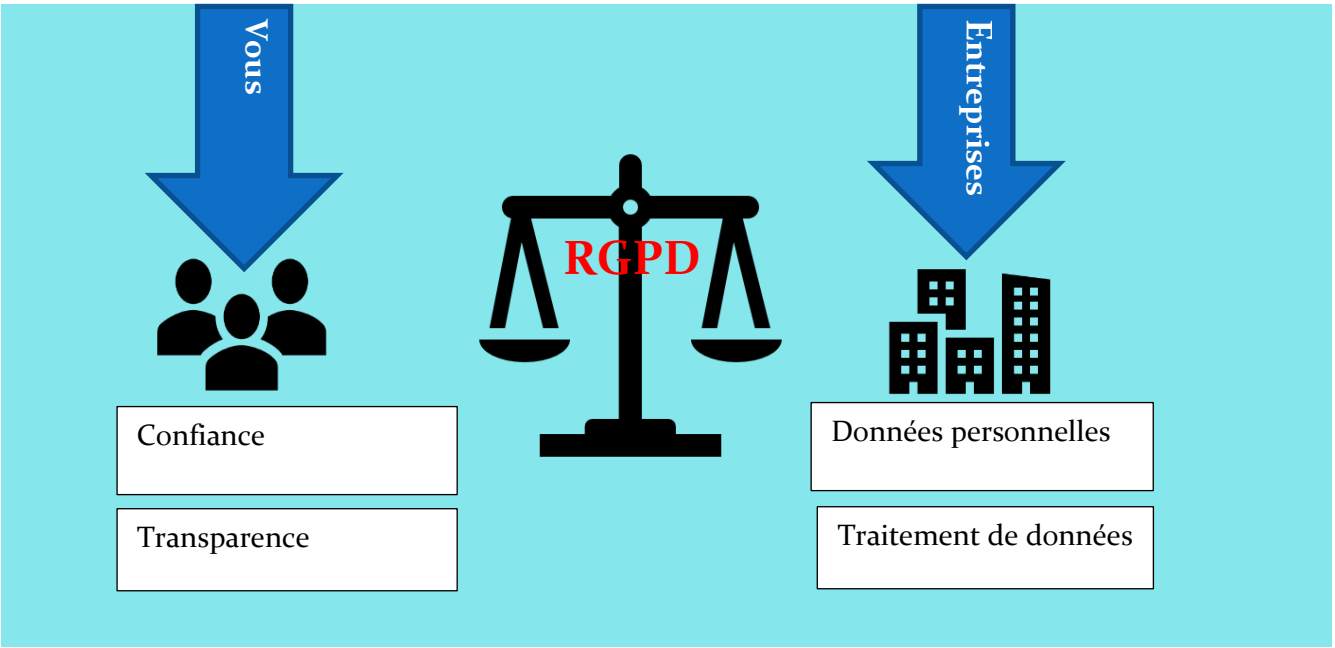
La norme RGPD

RGPD est le **R**ègle**G**lement **P**rotection **D**onnées, est le nouveau règlement européen sur la protection des données personnelle entrée en application le 25 mai 2018.

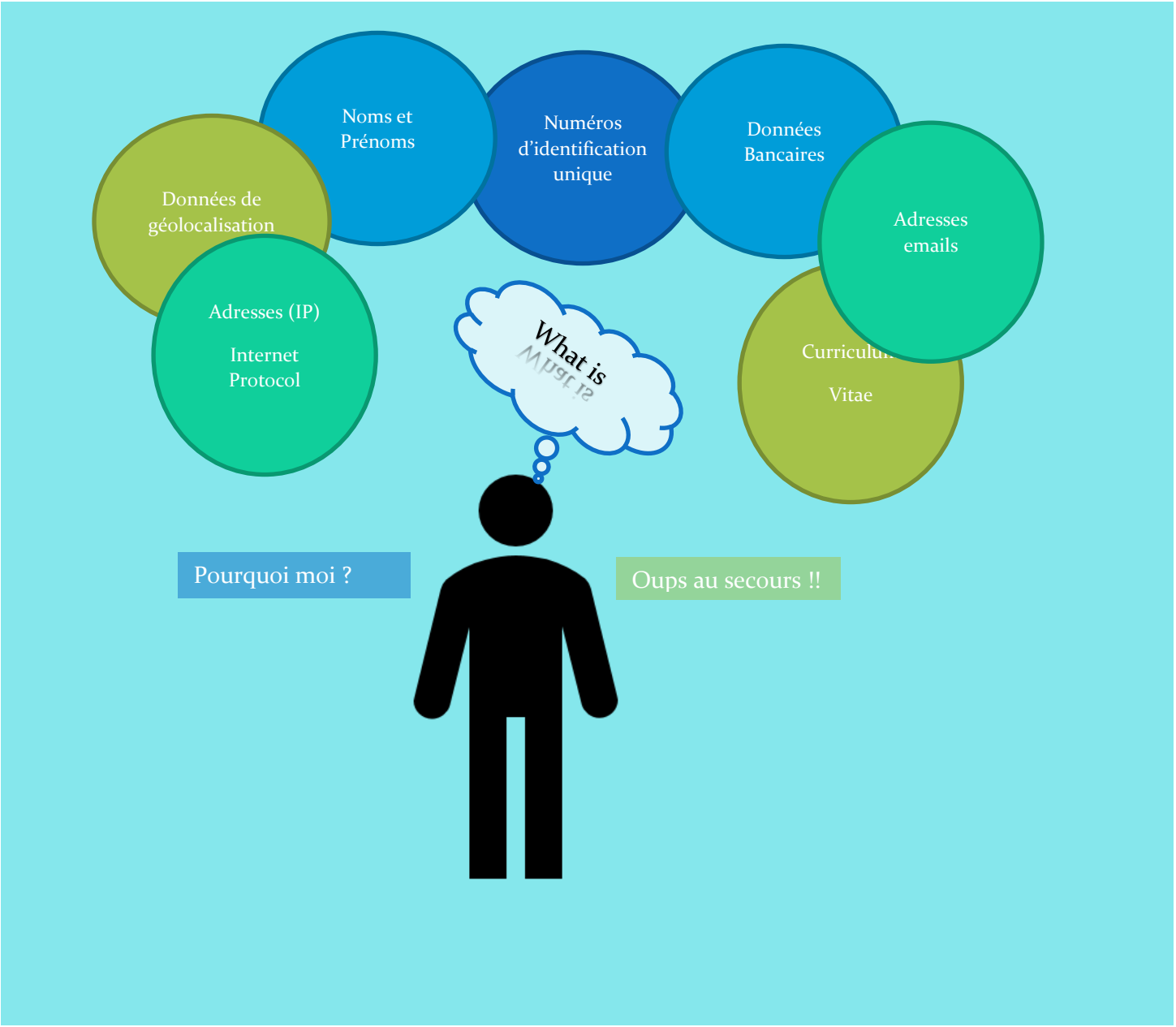
La réforme de la protection des données poursuit trois objectifs :

- Le renforcement des droits des personnes, notamment par la création d'un droit à la portabilité des données personnelles et de dispositions propres aux personnes mineures.
- Responsabiliser les acteurs traitant des données (responsables de traitement et sous-traitants) ;
- Crédibiliser la régulation grâce à une coopération renforcée entre les autorités de protection des données, qui pourront notamment adopter des décisions communes lorsque les traitements de données seront transnationaux et des sanctions renforcées.

En effet le nouvel règlement Européen impose une information concise, transparente, compréhensible, et aisément accessible des personnes concernées. (Défini aux articles 12, 13 et 14)



Les Données Personnelles



« Selon l'article 4 de la règlementation RGDP »

Les **Données Personnelles** correspondent aux informations relatives à une personne physique identifiée ou identifiable. Une personne naturelle identifiable est une personne qui peut être identifie

- Directement (Exemple : nom, prénom, adresse e-mails)
- Ou indirectement (Exemple : numéro d'identification unique ''numéro de sécurité sociale'', par un identifiant client, par la voix ou l'image…etc.) notamment par référence à un indicateur.

L'identification d'une **personne physique** peut être réalisée à partir de :

- Une seule donnée (exemple : numéro de sécurité sociale, ADN)
- Croissement d'un ensemble de données (exemple : adresse de localisation, date de naissance, abonnement à un magazine).

Les données personnelles à caractères sensible

Les données personnelles sensibles sont un ensemble spécifique de « catégories spéciales » qui doivent être traitées indépendamment des autres données personnelles avec une sécurité supplémentaire. Ces catégories sont :

- Origine raciale ou ethnique
- Opinions politiques
- Les croyances religieuses ou philosophiques
- L'adhésion à un syndicat
- Données génétiques
- Données biométriques (données traitées à des fins d'identification). Etc.

⚠ ***Important*** : Les données personnelles sensibles doivent être conservées séparément des autres données personnelles. Elles ne devraient être conservées que sur des périphériques mobiles que si le fichier a été chiffré.

La collecte des données personnelles

Les données personnelles peuvent être collectées de plusieurs manières, et à des fin multiples. Ci-dessous quelques moyens de collecte de ces données :

- La navigation sur des sites internet, engendre de nombreux cookies, qui pourront être utilisé à des buts commerciaux ou autres
- L'inscription de son CV sur un site de recherche d'emploi ou sur une CVThèque
- L'inscription ou la création de compte sur.....
- Participation à un sondage
- Achat sur un site de e-commerce
- Souscription à un magasine
- Ouverture de compte bancaire
- Abonnement téléphonique
- Inscription sur les réseaux sociaux
- Signature contrat de bail avec un promoteur immobilier
- Analyse dans un laboratoire de biologie médicale
- Récupération de données auprès de partenaire commerciaux.
- Les documents remis lors du processus d'Onbording dans une entreprise. Et plus encore.....etc.

La collecte de données personnelles peuvent donc être classée en deux grandes catégories dont :

- La collecte directe des données, données recueillies directement auprès des personnes
- La collecte indirecte des données, données recueillies indirectement auprès des personnes

La protection des données des citoyens Européen « one stop shop »

Une administration centralisée. Les entreprises sont désormais en contact avec un « guichet unique », à savoir l'autorité de protection des données de l'État membre où se trouve leur « établissement principal », désignée comme l'autorité « chef de file ».

Cet établissement est soit le lieu de leur siège central dans l'Union, soit l'établissement au sein duquel sont prises les décisions relatives aux finalités et aux modalités du traitement.

Les entreprises bénéficient ainsi d'un interlocuteur unique pour l'Union européenne en matière de protection des données personnelles, lorsqu'elles mettent en œuvre des traitements transnationaux.

Les analyses d'impact relatives à la protection AIP

Pour tous les traitements à risque, le responsable de traitement devra conduire une analyse d'impact complète, faisant apparaître les caractéristiques du traitement, les risques et les mesures adoptées. Concrètement, il s'agit notamment des traitements de données sensibles (données qui révèlent l'origine raciale ou ethnique, les opinions politiques, philosophiques ou religieuses, l'appartenance syndicale, les données concernant la santé ou l'orientation sexuelle, mais aussi, fait nouveau, les données génétiques ou biométriques), et de traitements reposant sur « l'évaluation systématique et approfondie d'aspects personnels des personnes physiques », c'est-à-dire notamment de profilage.

En cas de risque élevé, il devra consulter l'autorité de protection des données avant de mettre en œuvre ce traitement. Les « CNIL » pourront s'opposer au traitement à la lumière de ses caractéristiques et conséquences. (Source la CNIL)

La durée de rétention des données à caractères personnelles

Les données doivent être conservées pendant le plus court délai possible. Cette période devrait bien sûr tenir compte des raisons pour lesquelles votre entreprise doit traiter les données ainsi que des obligations juridiques qui vous imposent de garder les données pendant une période déterminée.

L'entreprise doit fixer des délais pour effacer ou examiner les données conservées.

Exceptionnellement, les données à caractères personnel peuvent être conservées plus longtemps à des fins archivistiques dans l'intérêts public ou à des fins de recherche scientifique ou historique……etc.

L'entreprise doit également s'assurer que les données qu'elle détient sont exactes et tenues à jour.

Reference : Article 5, paragraphe 1, point e) et considérant 39) du RGPD.

Le délégué à la protection des données alias DPD

Le délégué à la protection des données est le garant de la conformité des données au sein de l'entreprise. Il est principalement chargé de :

- Informer et de conseiller le responsable de traitement ou le sous-traitant, ainsi que leurs employés ;
- Contrôler le respect du règlement et du droit national en matière de protection des données ;
- Conseiller l'organisme sur la réalisation d'études d'impact sur la protection des données et d'en vérifier l'exécution.
- Coopérer avec l'autorité de contrôle et d'être le point de contact de celle-ci.

Afin de bien exécuter cette responsabilité, le DPO est tenue de :

- S'informer sur le contenu des nouvelles obligations
- Sensibiliser les décideurs sur l'impact de ces nouvelles règles
- Réaliser l'inventaire des traitements de données de votre organisme
- Concevoir des actions de sensibilisation ;
- Piloter la conformité en continu.

Les sanctions du non-respect de la norme RGPD

Les responsables de traitements et les sous-traitants peuvent faire l'Object de sanction administrative importante en cas du non-respect des règlements. Les sanctions suivantes peuvent être prononcées :

- Prononcer un avertissement ;
- Mettre en demeure l'entreprise ;
- Limiter temporairement ou définitivement un traitement ;
- Suspendre les flux de données ;

- Ordonner de satisfaire aux demandes d'exercice des droits des personnes ;
- Ordonner la rectification, la limitation ou l'effacement des données

S'agissant des amendes administratives, elles peuvent s'élever, selon la catégorie de l'infraction, de 10 ou 20 millions d'euros, ou, dans le cas d'une entreprise, **de 2% jusqu'à 4% du chiffre d'affaires annuel mondial**, le montant le plus élevé étant retenu.