Réponse d'Adan

Lignes directrices de l'EDPB sur le traitement des données personnelles par les technologies de la blockchain

L'Adan salue l'initiative du Conseil européen de la protection des données (EDPB) de fournir des orientations sur l'application du règlement général sur la protection des données (RGPD) aux technologies blockchain. Ces lignes directrices contribuent à un dialogue essentiel entre l'innovation et la réglementation, et l'Adan soutient l'objectif de veiller à ce que les systèmes basés sur la blockchain puissent fonctionner d'une manière respectueuse des droits fondamentaux et conforme aux normes juridiques européennes.

Toutefois, si les lignes directrices constituent une première étape précieuse, certaines recommandations soulèvent des préoccupations d'ordre juridique et pratique qui risquent de compromettre la capacité de l'Union européenne à soutenir le développement d'une infrastructure numérique souveraine et axée sur l'innovation. En particulier, l'interprétation des dispositions clés du GDPR - telles que la maîtrise des données, la qualification des données personnelles ou le droit à l'effacement - s'écarte parfois des principes de sécurité juridique, de neutralité technologique et de proportionnalité consacrés par le droit de l'UE. Plutôt que de chercher à rendre les technologies blockchain incompatibles avec le GDPR, l'objectif devrait être de clarifier les conditions dans lesquelles leur conception et leur fonctionnement peuvent être alignés sur le règlement. Il s'agit notamment de reconnaître que les obligations légales et les objectifs d'intérêt public (notamment la traçabilité ; la conformité ; et la prévention de la fraude) peuvent justifier la persistance de certaines données de manière sécurisée, décentralisée et transparente.

À cette fin, l'Adan propose d'envisager des exemptions spécifiques pour les validateurs et les acteurs techniques ou d'infrastructure, tels que les opérateurs de nœuds ou les mineurs, dont les rôles sont limités à des fonctions techniques telles que la validation des transactions et la maintenance du grand livre, sans déterminer les finalités ou les moyens du traitement des données. Ces exemptions reconnaîtraient le contrôle limité que ces acteurs exercent sur les données à caractère personnel, réduiraient les charges réglementaires excessives et favoriseraient la participation aux réseaux décentralisés, soutenant ainsi l'innovation tout en restant conformes à l'approche fondée sur les risques du GDPR. Une telle approche resterait pleinement cohérente avec la logique fondée sur les risques, contextuelle et équilibrée du GDPR.

La contribution d'Adan vise à mettre en évidence ces défis, à fournir une interprétation juridique constructive des dispositions pertinentes et à proposer des clarifications qui pourraient aider les lignes directrices à mieux refléter la réalité des infrastructures décentralisées et le rôle qu'elles peuvent jouer dans le soutien à l'innovation responsable au sein de l'économie numérique européenne.

*

Table des matières

1. Identification des responsables du traitement des données et des sous-traitants

1.1. Complexité de la définition des responsables du traitement des données en vertu de l'article 4, paragraphe 7

Un aspect essentiel de la conformité réglementaire consiste à identifier le responsable du traitement des données, chargé de veiller au respect des obligations prévues par le GDPR. Selon l'article 4, paragraphe 7, le responsable du traitement est la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement des données à caractère personnel.

Pour déterminer qui est le responsable du traitement des données, il est donc essentiel de déterminer qui décide des finalités (pourquoi) et des moyens (comment) des activités de traitement des données. Toutefois, les caractéristiques uniques de la blockchain mettent en évidence la complexité de la distinction entre les responsables du traitement des données et les sous-traitants. Les différents acteurs d'un écosystème de blockchain - tels que les nœuds, les mineurs, les utilisateurs eux-mêmes ou les structures de gouvernance - pourraient être considérés comme des responsables du traitement des données en fonction de leur rôle dans la détermination des moyens et des finalités du traitement des données.

Ces multiples acteurs peuvent assumer différentes fonctions, chacune pouvant influencer certains aspects des opérations du réseau. Cette architecture diffuse brouille la ligne de démarcation entre ceux qui décident des "finalités" du traitement, ce qui rend difficile l'attribution du rôle de responsable du traitement des données à une seule ou à plusieurs personnes physiques ou morales.

1.2. Opérateurs de nœuds et critères de contrôle

Au point 3.3, l'EDPB examine si les nœuds peuvent être considérés comme des responsables du traitement des données. La question de savoir si la responsabilité doit être attribuée aux opérateurs des nœuds est un sujet important qui mérite d'être approfondi.

La mesure dans laquelle les opérateurs de nœuds remplissent les critères de contrôle des données doit être évaluée au cas par cas, car souvent ils n'agissent pas intrinsèquement en tant que responsables du traitement des données au sens du GDPR. Si les nœuds stockent et transmettent des données de transaction, ils le font généralement dans le cadre du maintien de l'intégrité et de la sécurité du grand livre distribué, plutôt que dans l'intention d'analyser, de profiler ou d'utiliser activement ces données d'une manière qui s'apparente à celle d'un responsable du traitement.

En effet, leur rôle principal est de valider, de transmettre et de stocker les données de transaction, en veillant à ce que les transactions soient enregistrées conformément à des protocoles prédéfinis, souvent sans influence sur la finalité ou la portée des données traitées pour le transfert spécifique. En d'autres termes, leurs activités se limitent généralement à la

validation technique et à la propagation des transactions, plutôt qu'à la détermination des finalités du traitement des données à caractère personnel sous-jacentes contenues dans ces transactions. Dans ce cas, le rôle des nœuds n'est pas stratégique ni axé sur la finalité des données.

Étant donné que, selon le GDPR, le critère permettant de déterminer qui est le responsable du traitement des données exige la satisfaction des deux critères (décider de la finalité et des moyens), dans de nombreux cas, les opérateurs de nœuds pourraient être considérés comme des processeurs de données plutôt que comme des responsables du traitement des données.
Par conséquent, le niveau de contrôle et l'objectif du traitement des données nécessitent une analyse au cas par cas pour déterminer la maîtrise des données.

En particulier dans les systèmes de blockchain publics et sans permission, la détermination du contrôle devient complexe et nécessite une analyse contextuelle, au cas par cas. La principale difficulté réside dans le fait que, dans les réseaux décentralisés, aucun acteur n'exerce d'influence décisive sur les finalités et les moyens d'une manière conforme à la définition du contrôle du GDPR. Au contraire, la prise de décision peut être distribuée ou régie collectivement, ce qui complique l'attribution des responsabilités et de l'obligation de rendre compte du responsable du traitement. Dans ces contextes, les nœuds peuvent se contenter de traiter et de stocker les transactions conformément au protocole, sans définir les finalités réelles ou la nature des données concernées.

Au paragraphe 40, l'EDPB déclare de manière problématique : *Dans certains cas de blockchains publiques et sans permission, les nœuds n'agissent pas "au nom du contrôleur" et ne reçoivent aucune instruction d'un contrôleur ; au contraire**, ils peuvent, dans certains cas, décider de manière significative de modifier les objectifs et/ou les moyens essentiels pour poursuivre leurs propres objectifs*** *(par exemple, la décision de fork) en ce qui concerne les activités d'extraction et de validation. En ce sens, les nœuds peuvent soit exercer individuellement une influence décisive sur le sous-ensemble de transactions à ajouter au prochain bloc qu'ils extraient, soit en tant que groupe en acceptant (ou non) conjointement des modifications des protocoles et des règles à appliquer*.

Cette déclaration ne tient pas compte du fait que, dans les réseaux de blockchain, les décisions de bifurcation et autres sont généralement prises par la communauté ou par consensus. Les entités participantes se coordonnent ou se mettent d'accord sur la mise en œuvre d'une mise à jour du protocole, la modification des règles ou le soutien d'une chaîne alternative. Un seul nœud n'a généralement pas le pouvoir de créer ou de soutenir unilatéralement une fourche sans un consensus plus large, en particulier dans les réseaux décentralisés comme Ethereum.

D'une manière générale, l'acte de validation des transactions conformément aux règles du protocole ne doit pas se traduire par un exercice de détermination de l'objectif ou des moyens. Les nœuds traitent les données parce qu'ils y sont tenus par le protocole, et non parce qu'ils ont décidé de la raison d'être du traitement. Les finalités réelles et les intentions de traitement des données sont généralement définies par un organe de gouvernance

distinct, tel que les développeurs, les opérateurs ou les utilisateurs de la blockchain, plutôt que par les nœuds eux-mêmes.

Par exemple, la CNIL, l'autorité française de contrôle du GDPR, déclare que **les mineurs "*ne font que valider les transactions soumises par les participants*" et "*ne sont pas impliqués dans l'objet de ces transactions ; par conséquent, ils ne définissent pas les finalités et les moyens du traitement*"**.

Les lignes directrices proposent que les nœuds opérant sur des blockchains publiques et sans permission soient considérés comme des contrôleurs ou des co-contrôleurs au sens de la GRPD. Cependant, l'Adan fait respectueusement valoir que cette interprétation ne reflète pas fidèlement la fonction technique des nœuds.

Les nœuds valident passivement les transactions selon des protocoles de consensus prédéfinis et n'exercent pas de pouvoir discrétionnaire ni ne déterminent les finalités ou les moyens du traitement des données. Sur le plan fonctionnel, ils s'apparentent davantage à des routeurs de réseau qu'à des contrôleurs de données.

La classification des nœuds en tant que contrôleurs risque de décourager la participation à des systèmes décentralisés et pourrait par inadvertance saper les avantages en matière de protection de la vie privée que la décentralisation elle-même offre. L'Adan encourage l'EDPB à adopter une approche plus nuancée, au cas par cas, qui différencie les participants passifs à l'infrastructure des entités ayant un pouvoir de décision significatif sur le traitement des données personnelles.

Par conséquent, les lignes directrices devraient préciser que l'exploitation d'un nœud n'équivaut pas en soi à une fonction de contrôle. L'attribution des rôles GDPR devrait être basée sur l'influence et l'implication réelles d'une entité dans la détermination des finalités et des moyens du traitement. Cela peut être déterminé en réalisant une évaluation complète de l'impact sur la protection des données.

1.3. Gouvernance communautaire et prise de décision décentralisée

Si les lignes directrices soulignent à juste titre que certains acteurs, tels que les opérateurs de nœuds décrits à la section 1.2, peuvent parfois exercer une influence sur les opérations du réseau (par exemple, en participant à des forks ou à des changements de protocole), elles ne reconnaissent pas suffisamment les mécanismes de gouvernance alternatifs qui structurent la prise de décision dans les écosystèmes décentralisés. L'absence d'une entité juridique centralisée n'équivaut pas à un vide de gouvernance : au contraire, les réseaux de blockchain fonctionnent souvent dans des cadres de gouvernance collectifs, transparents et vérifiables impliquant les développeurs principaux, les DAO et les parties prenantes de la communauté au sens large.

Ce modèle de gouvernance distribuée reflète une forme légitime et de plus en plus reconnue de coordination organisationnelle, dans laquelle les décisions (y compris celles qui ont une incidence sur les finalités du traitement des données ou les changements de protocole) sont

prises dans le cadre de processus structurés et dirigés par la communauté. Il peut s'agir de votes en chaîne, de mécanismes de consensus ou de forums multipartites. **À ce titre, l'Adan considère que l'attribution des responsabilités liées au GDPR uniquement sous l'angle du contrôle hiérarchique traditionnel ne tient pas compte de ces nouveaux modèles et risque de fausser la réalité du contrôle et de la responsabilité dans les systèmes décentralisés.**

Par conséquent, l'Association recommande que les lignes directrices reconnaissent explicitement la gouvernance communautaire comme un facteur pertinent lors de l'évaluation de la fonction de contrôle et de la responsabilité au titre de l'article 4, paragraphe 7, du GDPR, en veillant à ce que l'interprétation juridique évolue au même rythme que l'innovation technologique et organisationnelle.

1.4. Les utilisateurs finaux en tant que contrôleurs potentiels

Les lignes directrices ne clarifient pas la question de savoir si les utilisateurs de données, qui sont également des personnes physiques, peuvent également exercer un contrôle sur les activités de traitement. Ce pouvoir de décision pourrait également appartenir aux utilisateurs finaux, qui pourraient spécifier quelles données sont téléchargées et pour quelles raisons.
Dans le contexte des activités du réseau de la blockchain, ce sont les individus qui déterminent l'objectif et la manière dont les données sont collectées conformément aux règles du protocole. Les validateurs et les nœuds n'exercent aucun pouvoir discrétionnaire ; plus précisément, ils n'exercent pas de pouvoir discrétionnaire significatif sur les finalités ou les moyens essentiels de traitement, mais suivent des règles déterministes définies par le protocole, et leurs actions sont purement techniques et procédurales. Par conséquent, les validateurs ne choisissent pas la manière dont les données sont structurées, stockées ou traitées ; ils ne peuvent pas se soustraire aux opérations imposées par le protocole sans cesser d'être des validateurs, et leur rôle consiste à appliquer mécaniquement un algorithme de consensus, et non à concevoir ou à modifier la logique de traitement des données.

Lorsqu'un utilisateur de données décide des types de données à caractère personnel à traiter, des objectifs du traitement, de la manière dont les données sont structurées et des personnes qui y ont accès, on peut considérer qu'il exerce un contrôle sur les activités de traitement et qu'il est donc considéré comme un responsable du traitement.

Bien que cela n'exclue pas qu'il puisse y avoir d'autres contrôleurs de données, dans le cas où, par exemple, une personne physique pourrait être considérée comme contrôleur de données, on ne sait toujours pas qui serait responsable de la mise en œuvre de la recommandation 3 selon laquelle les contrôleurs de données doivent informer les personnes concernées de la raison d'être du traitement, de l'existence de leurs droits et des modalités pour les exercer.

Alors que l'Adan affirme qu'une analyse au cas par cas est toujours nécessaire, les lignes directrices n'apportent pas d'éclaircissement à cet égard, alors que d'autres autorités nationales ont certainement abordé ce sujet.

Conformément aux critères énoncés à l'article 4, paragraphe 7, du GDPR, la CNIL française a observé que les participants, qui ont le droit d'écrire sur la chaîne et qui décident d'envoyer des données pour validation par les mineurs, peuvent être considérés comme des responsables du traitement des données. Parallèlement, l'article 2 dispose que le GDPR ne s'applique pas au traitement de données à caractère personnel effectué par une personne physique dans le cadre d'une activité purement personnelle ou domestique.

Selon la CNIL, les personnes physiques qui introduisent sur la blockchain des données à caractère personnel qui ne se rapportent pas à une activité professionnelle ou commerciale ne sont pas considérées comme des responsables de traitement et tombent sous le coup de l'exclusion *" activité purement personnelle ou domestique "* prévue à l'article 2 du RGPD.

La CNIL a souligné que : "*Par exemple, une personne physique qui achète ou vend des bitcoins, pour son propre compte, n'est pas un responsable de traitement. En revanche, cette personne peut être considérée comme un responsable de traitement si ces opérations sont réalisées dans le cadre d'une activité professionnelle ou commerciale, pour le compte d'autres personnes physiques*."

Dans le contexte des crypto-actifs, il s'agit d'un critère essentiel car, par exemple, un utilisateur qui initie une transaction en bitcoins peut être considéré comme le responsable du traitement des données impliquées dans cette transaction.

Au-delà des transferts de crypto-actifs, nous pourrions trouver d'autres exemples analogues dans lesquels les utilisateurs de données peuvent télécharger, gérer ou interagir avec des données sur une plateforme blockchain (qui ne se rapportent pas à une activité professionnelle ou commerciale).

D'une manière générale, il est essentiel d'identifier correctement le responsable de chaque activité de traitement de données à caractère personnel. Cela permet de clarifier vers qui les personnes concernées peuvent se tourner pour exercer leurs droits en vertu du règlement. Toutefois, dans le contexte des blockchains, cela devient particulièrement complexe.

Les multiples participants et acteurs opérant au sein du réseau peuvent jouer différents rôles, chacun influençant certains aspects du fonctionnement de la blockchain. Mais il est important de noter que ces rôles ne doivent pas nécessairement impliquer que chaque participant influence l'objectif principal du traitement des données lui-même.

Ainsi, **une vision extensive de la détermination de l'objet du traitement des données et de la personne qui fixe l'objectif risque d'étiqueter tous les participants à la blockchain comme des contrôleurs, ce qui crée une ambiguïté importante quant à la personne qui porte réellement la responsabilité finale.**

Cette ambiguïté complique encore la mise en œuvre de recommandations telles que l'obligation pour les responsables du traitement d'informer les personnes concernées

(recommandation 3). Déterminer qui doit fournir ces informations n'est pas clair lorsque la responsabilité est répartie entre de nombreux acteurs.

En outre, en vertu du GDPR, les responsables conjoints du traitement sont tenus d'établir des accords contractuels clairs pour définir les rôles et les responsabilités. Dans les modèles de gouvernance décentralisés et diffus typiques des écosystèmes de blockchain, la création de telles relations contractuelles devient non seulement peu pratique, mais souvent irréalisable. La nature même de la décentralisation présente des défis pour remplir les obligations du GDPR, telles que la réponse aux demandes d'accès, d'effacement ou de portabilité des personnes concernées.

Les technologies blockchain et les écosystèmes numériques décentralisés modifient fondamentalement les paradigmes traditionnels de gestion et de gouvernance des données. La nature décentralisée et distribuée rend difficile l'identification d'un contrôleur unique et identifiable. Cette décentralisation rend difficile l'identification d'un seul contrôleur de données responsable de la conformité au GDPR, car de multiples participants peuvent influencer les décisions de traitement collectivement ou indépendamment, en particulier dans les environnements sans permission.

Par conséquent, les lignes directrices actuelles du GDPR peinent souvent à s'appliquer clairement à ces nouvelles structures décentralisées, ce qui entraîne une ambiguïté dans l'attribution des responsabilités en matière de respect des droits des personnes concernées.

2. Qualification des "données à caractère personnel

La définition des données à caractère personnel au titre de l'article 4, paragraphe 1, du GDPR est intentionnellement large. Elle englobe toute information concernant une personne physique identifiée ou identifiable (directement ou indirectement) et comprend des identifiants tels que les noms, les numéros d'identification, les données de localisation ou "*les éléments spécifiques à l'identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale de cette personne*".

Dans les réseaux de blockchain, certains types de données, y compris, mais sans s'y limiter, les clés publiques, les informations hachées et les métadonnées des transactions, **ne sont pas intrinsèquement personnelles, mais peuvent devenir des données personnelles lorsqu'elles se rapportent à une personne identifiable**, soit seules, soit en combinaison avec d'autres données. Cette position est reflétée dans les orientations de l'EDPB et confirmée par les autorités de contrôle nationales telles que la CNIL.

Le critère clé (*voir le* considérant 26, GRPD) est de savoir si une personne est identifiable "*par des moyens raisonnablement susceptibles d'être utilisés*", en tenant compte de tous les facteurs objectifs (coûts, temps et technologie disponible). En pratique, cela signifie que même les identifiants pseudonymes, tels que les adresses de blockchain ou les valeurs

hachées, peuvent relever du champ d'application des données à caractère personnel s'ils peuvent être liés à une personne physique grâce à des informations contextuelles.

Par exemple, une adresse publique utilisée à plusieurs reprises dans des transactions ou partagée sur un forum peut être associée à un profil d'utilisateur, ce qui rend les données "relatives" à cette personne. De même, un hachage de données personnelles peut conserver son caractère identifiable si les données sous-jacentes sont connues ou devinables.

L'Adan ne conteste pas que les clés publiques et les hachages peuvent, dans certains cas, être qualifiés de données à caractère personnel. Toutefois, cette qualification dépend du contexte réel et du risque d'identifiabilité, et non du seul format technique. **Les mêmes données peuvent ou non être personnelles en fonction de la manière dont elles sont générées, combinées et utilisées dans la pratique**.

Bien que nous soyons d'avis qu'une adresse de portefeuille n'est pas une donnée à caractère personnel au sens du GDPR lorsqu'elle ne permet pas d'identifier la personne concernée, il est important d'examiner comment nous analyserions la question si une adresse de portefeuille était également considérée comme une donnée à caractère personnel. Une partie intégrante de l'analyse consiste à comprendre que lorsqu'un utilisateur utilise la blockchain pour une transaction, il choisit intrinsèquement et volontairement de partager ses données sur un grand livre public. L'utilisateur a consenti à ce que ses données existent sur la blockchain lorsqu'il a effectué la transaction, et maintenant, pour maintenir les opérations et l'intégrité de la blockchain, la partie contrôlante aurait un intérêt légitime à conserver ces données dans le grand livre public.

Ensuite, Adan exhorte l'EDPB à éviter une vision formaliste ou "statique" de l'"identifiabilité". Une interprétation plus nuancée et contextuelle est nécessaire pour refléter les réalités techniques des systèmes de blockchain.

En effet, le seuil d'identifiabilité, et donc la détermination du caractère "personnel" des données, dépend du contexte et peut varier considérablement en fonction des ensembles de données disponibles, des outils d'analyse et des capacités des acteurs.

Les lignes directrices pourraient explicitement encourager une analyse contextuelle fondée sur le risque pour déterminer si les données sont "*personnelles*" dans un scénario donné. Par exemple, une clé publique peut être considérée comme une donnée personnelle dans une application DeFi de vente au détail avec des identifiants persistants, mais pas dans une couche d'infrastructure purement technique où les clés font l'objet d'une rotation fréquente et où il n'y a pas de profilage externe.

La possibilité d'établir un lien entre les données de la chaîne et les identités hors chaîne est un vecteur de risque essentiel. Même lorsque seules des données hachées ou pseudonymisées sont stockées sur la chaîne, une réidentification peut toujours être possible par le biais d'une corrélation de données externes ou d'une analyse des schémas comportementaux. **L'Association recommande donc que les lignes directrices fournissent**

des exemples concrets de ce qui constitue une pseudonymisation suffisante dans le cadre de la blockchain, et qu'elles la différencient de l'anonymisation, qui est rarement réalisable sur la chaîne.

Les lignes directrices devraient également reconnaître la distinction entre les "*identificateurs fonctionnels*" et les identificateurs personnels traditionnels, et donc suggérer des mesures de conception plus appropriées pour minimiser le risque d'identifiabilité (par exemple, rotation des adresses, ZKP, mixers....).

L'Adan estime que les lignes directrices bénéficieraient d'un traitement plus approfondi de la question suivante : qu'est-ce qui constitue des données à caractère personnel dans les contextes de blockchain ? Les systèmes de blockchain, en particulier les systèmes publics sans permission, reposent souvent sur des identifiants cryptographiques (*par exemple, des* adresses de portefeuilles, des hachages de transactions ou des interactions de contrats intelligents) qui peuvent ne pas identifier directement les individus, mais pourraient être liés à eux par le biais de données auxiliaires. Pour plus de clarté, l'Adan recommande que l'EDPB fournisse des orientations supplémentaires sur l'évaluation de l'identifiabilité dans les contextes de blockchain, y compris un spectre d'exemples allant de cas clairs de données personnelles à des données pseudonymes ou hachées à la limite de l'identifiabilité. Cela aidera les développeurs, les professionnels de la protection de la vie privée et les régulateurs à appliquer les exigences du GDPR de manière plus cohérente et proportionnée.

Si la définition des "données personnelles" est appliquée de manière trop large et sans proportionnalité, même non intrusive ou préservant la vie privée, les utilisations de la blockchain peuvent être capturées sans nécessairement être soumises aux obligations du GDPR. Cela risque de créer des effets de refroidissement réglementaire, d'étouffer l'innovation et de décourager l'adoption de pratiques de décentralisation bénéfiques. Une interprétation équilibrée, fondée sur les réalités techniques et le risque réel de réidentification, favoriserait une conformité plus pragmatique**.**

3. Obligation d'effacement et de suppression de l'ensemble de la blockchain

3.1. Fragmentation architecturale et responsabilité

L'une des principales difficultés liées à la mise en œuvre de ces lignes directrices est la difficulté de déterminer qui doit être tenu responsable de la sauvegarde des droits des personnes concernées, en particulier lorsqu'il s'agit de responsabilités telles que le droit à l'effacement.

Les modèles de réseau supposés par les lignes directrices semblent dépassés, présentant des scénarios dans lesquels un réseau de blockchain unique et unifié gère l'ensemble des opérations de traitement des données. Dans la pratique, les écosystèmes de blockchain sont décentralisés et de plus en plus modulaires, impliquant de multiples réseaux et acteurs remplissant différentes fonctions telles que l'exécution, le consensus ou le stockage de données.

La décentralisation ne doit donc pas être envisagée uniquement sous l'angle du pouvoir de décision (qui fixe les objectifs de traitement des données), mais aussi sous l'angle de la division fonctionnelle, où différentes entités s'occupent d'aspects distincts, mais interconnectés, de la gestion des données.

Cette diversité signifie que **les rôles sont répartis entre diverses entités,** certaines étant des personnes individuelles, d'autres des entités, chacune s'occupant de divers aspects du cycle de vie du processus de données. La notion de contrôleur ou d'entité responsable ne correspond pas nécessairement à la réalité opérationnelle de nombreux réseaux blockchain, en particulier ceux qui sont construits sur des architectures modulaires, où les responsabilités sont réparties et où aucune entité n'a une supervision complète de l'ensemble du processus de gestion des données.

Cette fragmentation intensifie les défis liés au respect des droits des personnes concernées, en particulier le droit à l'effacement, car il n'est pas toujours évident de savoir quel acteur a l'autorité ou la capacité de répondre (en solo) à de telles demandes. Comme indiqué précédemment, ce défi est accentué par une interprétation large de ce qui constitue un objectif de traitement des données et de qui est responsable de la définition de cet objectif, ce qui entraîne une responsabilité ambiguë qui ne correspond pas bien aux rôles généralement envisagés dans le cadre du GDPR. Cette fragmentation remet en question les notions "traditionnelles" de responsabilité, ce qui rend le respect des droits en matière de confidentialité des données dans les environnements blockchain décentralisés et modulaires beaucoup plus complexe que dans les systèmes conventionnels et centralisés.

Cette difficulté est également illustrée par l'approche des lignes directrices en matière de mécanismes de responsabilité, notamment en ce qui concerne la tenue d'un registre des activités de traitement au titre de l'article 30 du GDPR.

> La section 3.4. p.112 des lignes directrices indique qu'*"un registre des activités de traitement doit être tenu conformément à l'article 30 du GDPR. Il ne suffit pas de prétendre que, parce que la blockchain est décentralisée, personne n'est chargé de tenir un tel registre."*

Toutefois, cette déclaration ne reflète pas les réalités opérationnelles et de gouvernance des écosystèmes de blockchain décentralisés, où aucune entité ne peut avoir la capacité, ni même la légitimité, de tenir un tel registre au nom de l'ensemble du réseau, comme décrit ci-dessus.

Si le principe de responsabilité reste pleinement applicable, sa mise en œuvre peut différer dans les contextes décentralisés. Par exemple, de nombreux projets peuvent s'appuyer sur des contrats intelligents qui auto-déclarent certains paramètres de traitement des données, ou sur des interfaces publiques gérées par la communauté pour décrire les structures de données, les règles d'accès ou la logique de conservation. Ces outils de conformité

décentralisés et souvent open-source offrent des niveaux significatifs de transparence, de traçabilité et d'information des utilisateurs.

L'Adan recommande donc que les lignes directrices reconnaissent la possibilité de cadres de responsabilité distribués ou décentralisés, à condition qu'ils permettent une documentation efficace, une surveillance réglementaire et la protection des utilisateurs.
Les contrats intelligents peuvent automatiser des décisions qui peuvent avoir des effets juridiques ou significatifs sur les individus, invoquant potentiellement l'article 22 du GDPR. L'EDPB devrait offrir des conseils pour garantir la transparence, la contestabilité et la surveillance humaine dans les déploiements de contrats intelligents qui traitent des données à caractère personnel.

La reconnaissance de ces mécanismes resterait pleinement cohérente avec la logique du GDPR axée sur les résultats et refléterait mieux la diversité des modèles de conformité émergeant dans les environnements décentralisés.

3.2. Minimisation des données et stockage hors chaîne

L'Adan soutient les orientations de l'EDPB préconisant la minimisation des données et l'évitement du stockage de données personnelles directement sur la blockchain. Ce principe est particulièrement vital étant donné l'immuabilité des grands livres de la blockchain, qui peuvent rendre toute inclusion de données personnelles effectivement permanente et inaccessible à la modification ou à la suppression.

De nombreux fournisseurs de services utilisent des solutions de stockage hors chaîne pour héberger toutes les données susceptibles d'être liées à des personnes identifiables, en ne stockant que des pointeurs hachés ou des identifiants sur la chaîne afin de maintenir la fonctionnalité nécessaire sans compromettre la vie privée.

Toutefois, il serait utile que les lignes directrices soient davantage développées dans ces domaines clés :

- **Normalisation des architectures hors chaîne** : alors que de nombreux fournisseurs de services de blockchain adoptent le stockage hors chaîne pour rester conformes au GDPR, l'absence de normes harmonisées entraîne des mises en œuvre incohérentes et des risques de sécurité potentiels.
- **Risques de liaison et de réversibilité** : même lorsque seules des données hachées ou pseudonymisées sont stockées sur la chaîne, il subsiste un risque de réidentification, en particulier lorsque ces données peuvent être reliées à des ensembles de données ou à des métadonnées hors chaîne.

L'Adan préconise des orientations plus concrètes ou un alignement sur les cadres existants (par exemple, ISO/IEC 27001, NIST) pour garantir que les environnements hors chaîne atteignent un seuil approprié en matière de protection et de sécurité des données.

Les lignes directrices pourraient bénéficier d'une analyse plus approfondie des risques résiduels posés par la possibilité d'établir des liens et de recommandations pour des garanties appropriées, telles que des engagements cryptographiques ou des preuves à connaissance nulle (ZKP).

3.3. Transferts internationaux de données

L'Adan salue l'inclusion par l'EDPB de considérations relatives au transfert international de données dans le contexte des réseaux de blockchain, où les nœuds peuvent être géographiquement dispersés et où le flux de données transcende souvent les frontières juridictionnelles.
Cependant, l'application pratique du *chapitre V* du GDPR aux environnements blockchain décentralisés reste ambiguë et présente des défis de conformité substantiels. Dans les architectures traditionnelles, les exportateurs de données peuvent identifier les destinataires, évaluer l'environnement juridique du pays tiers et mettre en œuvre des garanties appropriées telles que les clauses contractuelles types (CCN) ou les règles contraignantes pour les entreprises (BCR). En revanche, les participants à la blockchain, en particulier dans les réseaux publics sans autorisation, ne peuvent pas facilement identifier où se trouvent les nœuds, ni qui les contrôle, ce qui rend presque impossible de déterminer si un transfert a eu lieu, et encore moins d'établir un mécanisme légal à cet effet.

Voici donc les principaux défis et domaines à clarifier :

- **Définition du "transfert" dans les systèmes décentralisés :**
  - Les lignes directrices gagneraient à définir plus précisément ce qui constitue un "transfert" dans le cadre de la blockchain. Par exemple, s'agit-il d'un transfert lorsqu'une transaction est validée par un nœud situé dans un pays tiers, même si la transaction a été initiée au sein de l'EEE ? Une plus grande clarté sur le moment et la manière dont l'activité de la blockchain déclenche le régime de transfert favoriserait une application cohérente des obligations du GDPR.
- **Applicabilité des mécanismes de transfert (par exemple, CCN, BCR) :**
  - Les mécanismes actuels de transfert international de données ont été conçus pour des échanges de données centralisés. Leur application dans des réseaux ouverts, où les données peuvent être propagées à des entités inconnues dans des juridictions inconnues, est très peu pratique. Les lignes directrices devraient reconnaître cette lacune et fournir des solutions provisoires ou approuver des approches alternatives (par exemple, des obligations contractuelles au niveau de la couche d'application, des restrictions d'accès techniques ou une séparation architecturale entre les nœuds de l'EEE et les nœuds hors EEE).
- **Approche de la validation globale basée sur le risque :**
  - Dans de nombreux cas d'utilisation de la blockchain, les données sur la chaîne sont soit pseudonymisées, soit rendues non personnelles par le biais de stratégies de conception robustes (par exemple, *en* ne stockant

que des hachages ou des valeurs cryptées). Dans de tels contextes, les risques traditionnellement associés aux transferts internationaux sont considérablement réduits. Nous encourageons l'EDPB à adopter une perspective proportionnelle, basée sur le risque, lorsqu'elle envisage l'application des règles de transfert pour les systèmes de blockchain.

- **Soutien aux conceptions de réseaux renforçant la protection de la vie privée** :
    - Les conceptions émergentes de la blockchain, telles que les réseaux autorisés avec contrôle des nœuds géographiques ou les chaînes de consortium avec des restrictions juridictionnelles appliquées, offrent des voies pratiques pour la conformité des transferts. Les lignes directrices pourraient les mettre en avant en tant qu'exemples de bonnes pratiques, en encourageant la conception d'architectures respectueuses de la vie privée.

Par conséquent, l'Adan recommande à l'EDPB de fournir plus de clarté sur la façon dont les règles de transfert international s'appliquent aux réseaux décentralisés, et d'explorer le développement de cadres de conformité de transfert spécifiquement adaptés aux systèmes de blockchain. En outre, l'EDPB devrait envisager de reconnaître la valeur des mesures techniques et organisationnelles qui réduisent la réidentification et l'exposition transfrontalière dans le cadre d'une évaluation proportionnée basée sur le risque.

3.4. Évaluations de l'impact de la protection des données (DPIA)

L'Adan soutient fortement l'accent mis par l'EDPB sur la réalisation d'évaluations de l'impact sur la protection des données (DPIA) pour les activités de traitement basées sur la blockchain. Compte tenu de la nature innovante et souvent complexe des systèmes de blockchain, les DPIA servent d'outil essentiel pour identifier, évaluer et atténuer les risques liés à la protection des données dès le début du processus de conception, en s'alignant sur les principes de la protection de la vie privée dès la conception et par défaut (article 25 du GDPR). Cependant, nous pensons que les lignes directrices bénéficieraient d'une spécificité supplémentaire concernant la façon dont les DPIA devraient être adaptés aux contextes de la blockchain, en particulier lorsque les hypothèses conventionnelles de contrôle, de centralisation et de gestion du cycle de vie des données ne tiennent pas.

Pour améliorer la conformité pratique, l'EDPB devrait fournir des orientations sur la prise en compte des risques spécifiques à la blockchain qui sont souvent absents des modèles d'EDPI ou des bibliothèques de risques existants. Par exemple, l'irréversibilité de l'enregistrement des données, l'absence de gouvernance centrale et le potentiel de liaison ou de réidentification des données pseudonymes présentent des défis uniques. Ces risques sont particulièrement prononcés dans des scénarios tels que l'utilisation de contrats intelligents pour la prise de décision automatisée, le stockage de métadonnées sur la chaîne, ou la réplication de données entre des nœuds dans plusieurs juridictions. Proposer des évaluations de risques typiques et des options d'atténuation pour ces scénarios aiderait les organisations à concevoir des systèmes conformes à la protection de la vie privée. De même, dans les réseaux de blockchain sans permission ou dirigés par un consortium, où aucune entité ne contrôle entièrement le traitement des données, les DPIA doivent tenir

compte des modèles de gouvernance partagée. Les lignes directrices devraient préciser comment documenter les risques résiduels de manière transparente lorsque les mesures d'atténuation ne peuvent pas être entièrement mises en œuvre par un seul acteur et encourager la collaboration entre les entités, par exemple par le biais de DPIA conjointes ou de cadres de gouvernance coopératifs.

En outre, l'EDPB pourrait rationaliser le processus d'AIPD en recommandant des critères de sélection adaptés aux systèmes de technologie du grand livre distribué afin de déterminer si une AIPD est nécessaire. Des questions telles que l'inscription directe ou indirecte de données à caractère personnel dans la blockchain, le déclenchement par des contrats intelligents d'actions automatisées ayant des effets juridiques ou significatifs, ou le fonctionnement de nœuds dans des pays tiers sans décisions adéquates, aideraient les organisations à évaluer la nécessité d'une DPIA dès le début de la phase de conception. En outre, des DPIA efficaces pour les projets de blockchain nécessitent une collaboration interfonctionnelle. Les professionnels de la protection de la vie privée doivent travailler en étroite collaboration avec les architectes de systèmes, les développeurs de contrats intelligents et les concepteurs de réseaux pour s'assurer que les risques sont correctement compris et atténués. Les lignes directrices devraient préconiser l'intégration des processus de DPIA dans les cycles agiles et DevOps, en particulier dans l'environnement Web3 en évolution rapide, afin de favoriser des pratiques de développement respectueuses de la vie privée.

L'Adan exhorte l'EDPB à élaborer ou à approuver des orientations et des modèles d'EDPI spécifiquement adaptés aux applications blockchain. Ceux-ci devraient aborder les défis techniques et de gouvernance uniques des systèmes décentralisés, promouvoir l'identification normalisée des risques et fournir des conseils pratiques sur la documentation des stratégies d'atténuation, même en l'absence d'un contrôle total sur l'écosystème de traitement.

3.5. Immuabilité et droits des personnes concernées

L'Adan apprécie que l'EDPB reconnaisse la tension entre l'immutabilité inhérente à la blockchain et l'exercice des droits des personnes concernées en vertu du GDPR, en particulier les droits à la rectification (article 16) et à l'effacement (article 17). Si les lignes directrices préconisent à juste titre le stockage hors chaîne des données à caractère personnel en tant que mesure d'atténuation pratique, il est nécessaire de clarifier davantage la manière de traiter les risques résiduels et les exceptions, en particulier lorsque les données à caractère personnel peuvent être écrites sur la chaîne par inadvertance ou à la suite d'actions de l'utilisateur échappant au contrôle du fournisseur de services.

Dans les environnements blockchain publics et sans permission, où tout participant peut écrire dans le grand livre, il est techniquement difficile d'empêcher l'inclusion de données personnelles. Par exemple, les métadonnées intégrées dans les transactions, telles que les adresses de portefeuille, les données liées à l'IP ou le contenu généré par l'utilisateur, peuvent contenir ou déduire des données personnelles. De même, les contrats intelligents

peuvent encoder des termes ou des identifiants spécifiques à l'utilisateur qui sont gravés de manière permanente dans la chaîne. **Ces réalités posent un dilemme opérationnel : une fois que les données personnelles sont sur la chaîne, elles ne peuvent être modifiées ou supprimées sans porter atteinte à la structure fondamentale et au modèle de confiance de la blockchain**. Cependant, des suggestions telles que "supprimer toute la blockchain" ne sont pas utiles au secteur et ne répondent pas aux besoins pratiques de conformité.

Pour aider les parties prenantes à relever ces défis, l'EDPB devrait préciser comment l'"effacement effectif" peut être interprété dans des contextes où l'effacement est techniquement impossible. Par exemple, rendre les données inaccessibles par des méthodes telles que la suppression des clés ou l'obscurcissement cryptographique pourrait, dans certains scénarios, répondre à l'intention de l'article 17. Une position plus définitive sur ces approches guiderait les contrôleurs dans le développement d'architectures de blockchain conformes. En outre, les technologies émergentes de préservation de la vie privée, telles que les hachages caméléon, les zk-SNARK et les schémas "commit-reveal", offrent des moyens prometteurs de concilier l'immutabilité avec les exigences du GDPR. Bien qu'elles ne soient pas encore courantes, la reconnaissance de leur potentiel par l'EDPB pourrait encourager l'innovation et accélérer leur adoption dans les écosystèmes de la blockchain.

Les lignes directrices devraient traiter de manière plus nuancée la question de savoir si toutes les informations sur la chaîne, telles que les adresses pseudonymes, les hachages de transactions ou les identifiants de contrats intelligents, devraient être traitées comme des données à caractère personnel en tant que telles, ou si des seuils de contexte et de réidentifiabilité devraient s'appliquer. Distinguer les données personnelles et les métadonnées en fonction de leur risque d'identifiabilité permettrait aux parties prenantes d'évaluer les obligations de conformité de manière proportionnée et d'éviter des interprétations trop larges qui pourraient étouffer l'innovation.
L'Adan demande instamment à l'EDPB de fournir des orientations interprétatives supplémentaires sur la manière dont les droits des personnes concernées, en particulier l'effacement et la rectification, peuvent être respectés dans des environnements immuables, y compris par des moyens techniques alternatifs. En outre, l'Association recommande que les lignes directrices promeuvent une approche basée sur le risque et la proportionnalité qui reconnaisse les limites techniques des systèmes décentralisés tout en encourageant les garanties innovantes en matière de protection de la vie privée.

3.6. Suppression de l'ensemble de la blockchain et proportionnalité juridique

3.6.1. Caractère conditionnel du droit à l'effacement

Selon les lignes directrices, une fois ces objectifs atteints, les données doivent être rendues anonymes ou supprimées. Le paragraphe 63 précise que lorsque la suppression n'a pas été prise en compte dès la conception, il peut être nécessaire de supprimer l'ensemble de la blockchain.

Une telle conclusion semble reposer sur une lecture partielle de l'article 17 du GDPR, qui consacre le "*droit à l'effacement*". En vertu de l'article 17, paragraphe 1, la personne concernée a le droit d'obtenir l'effacement des données à caractère personnel la concernant "*sans retard injustifié*", mais uniquement si l'un des motifs juridiques limités est satisfait. Il s'agit notamment du fait que les données ne sont plus nécessaires au regard des finalités pour lesquelles elles ont été collectées **(a)**, que la personne concernée retire son consentement **(b)** ou que les données ont fait l'objet d'un traitement illicite **(d)**. **Par conséquent, le droit à l'effacement n'est pas absolu mais conditionnel.**

L'article 17, paragraphe 3, prévoit explicitement les circonstances dans lesquelles ce droit ne s'applique pas. En particulier, l'article 17, paragraphe 3, point b), dispose que le droit à l'effacement ne s'applique pas lorsque le traitement est nécessaire au respect d'une obligation légale ou à l'exécution d'une mission d'intérêt public. Ces exceptions sont particulièrement pertinentes dans le contexte des blockchains, qui peuvent servir des objectifs liés à l'intérêt public ou au respect de la loi (sans se limiter aux cas d'utilisation réglementés). Le stockage continu de données sur une blockchain peut donc être non seulement légitime, mais également requis par la loi, y compris dans divers contextes tels que la sécurité juridique, la traçabilité ou la prévention de l'utilisation abusive.

Ensuite, l'interprétation de l'article 17 comme imposant la suppression en bloc d'une blockchain entière - en particulier lorsqu'aucun mécanisme d'effacement n'a été prévu à la conception - ne tient pas compte de l'architecture juridique du GDPR. Le règlement établit un équilibre entre les droits des personnes concernées et d'autres obligations légales ou d'intérêt public. Exiger l'effacement "*chaque fois que l'effacement n'a pas été envisagé dès la conception*" reviendrait à imposer une obligation qui n'est ni fondée sur la lettre du GDPR ni cohérente avec sa logique de proportionnalité.

3.6.2. Restrictions admissibles au droit d'effacement

L'Adan considère que cette interprétation rigide néglige également l'article 23 du GDPR, qui permet au droit de l'Union ou de l'État membre (EM) de restreindre les droits des personnes concernées - et notamment l'article 17 - lorsque ces restrictions sont nécessaires et proportionnées pour sauvegarder des objectifs tels que la prévention des infractions pénales ou la protection d'intérêts économiques ou financiers importants. Ces limitations sont essentielles lorsqu'il s'agit d'évaluer comment les droits de protection des données s'appliquent au sein d'infrastructures décentralisées, transparentes et immuables telles que les blockchains.

En ce sens, l'Association souligne que la transparence est l'une des principales caractéristiques et propositions de valeur de la technologie blockchain, souvent considérée comme un moyen d'instaurer la confiance et la responsabilité pour les activités menées sur le réseau. Bien que nous soyons d'accord sur le fait que les données des utilisateurs devraient toujours être protégées, l'adoption d'une telle approche tout ou rien pour la suppression peut créer des complexités supplémentaires pour les utilisateurs et les entreprises qui vont au-delà des discussions sur la protection des données.

Nous convenons que les données des utilisateurs doivent être protégées à tout moment, mais une approche aussi sévère pourrait également introduire d'autres complexités, potentiellement préjudiciables aux entreprises et aux utilisateurs eux-mêmes dans d'autres aspects que les raisons de protection des données. Les blockchains permettent la transparence, et la transparence permet de rendre des comptes. Et cette transparence et cette responsabilité peuvent être nécessaires dans d'autres contextes, y compris d'un point de vue réglementaire.

3.6.3. Pertinence pour la surveillance réglementaire et la conformité aux règles de lutte contre le blanchiment d'argent

Bien que la suppression de la blockchain puisse sembler attrayante du point de vue de la protection de la vie privée ou de la minimisation des données, elle se heurte fondamentalement au cadre juridique et réglementaire mis en place pour prévenir les activités illicites et garantir que les autorités puissent exercer efficacement leurs fonctions de contrôle.

Du point de vue de la surveillance, les autorités ont souvent besoin d'accéder à l'historique des transactions et aux données des utilisateurs pour surveiller et enquêter sur des activités suspectes liées à des problèmes de lutte contre le blanchiment d'argent. Si l'ensemble de la blockchain devait être supprimé, il n'y aurait plus d'enregistrements sur lesquels les régulateurs s'appuient pour les contrôles de conformité et les enquêtes.

Les données contenues dans la blockchain permettent également aux outils analytiques sophistiqués de la blockchain de retracer les flux de fonds illicites, d'identifier les activités illicites potentielles et les schémas suspects, contribuant ainsi à démasquer les réseaux criminels. Par conséquent, cela entraverait gravement les efforts d'application de la loi, affaiblirait la transparence et diminuerait potentiellement la capacité à se conformer aux obligations légales.

La transparence de la blockchain est l'un de ses plus grands avantages dans la lutte contre la criminalité financière et elle a un effet dissuasif sur les mauvais acteurs en raison de la capacité des forces de l'ordre à retracer les transactions illicites.

Il est important de noter qu'**en vertu de la législation de l'UE, les entités obligées sont tenues de mettre en œuvre des mesures de diligence raisonnable en matière de lutte contre le blanchiment d'argent, qui comprennent la surveillance continue des transactions, l'analyse des schémas et la déclaration en temps opportun des activités suspectes aux autorités. La suppression des données sur la blockchain les empêcherait essentiellement de remplir ces obligations, ce qui rendrait la surveillance inefficace et disproportionnée par rapport aux risques encourus. En outre, cette suppression pourrait créer d'importantes zones d'ombre, permettant aux acteurs malveillants d'exploiter l'absence d'enregistrements pour dissimuler leurs actions, ce qui compromettrait l'objectif même des réglementations en matière de lutte contre le blanchiment d'argent et faciliterait potentiellement les** activités **criminelles**.

4. Absence de neutralité technologique

Le paragraphe 49 des lignes directrices suggère que les blockchains publiques ne devraient être employées que si l'accès public au grand livre est nécessaire pour au moins l'une des finalités du traitement. Cette formulation soulève d'importantes préoccupations car elle s'écarte du principe de neutralité technologique, qui est un élément fondamental du droit et de la politique de l'UE - y compris dans le domaine de la protection des données. Le GDPR ne prescrit ni ne favorise aucune technologie spécifique, pas plus qu'il ne limite les moyens par lesquels les activités de traitement des données peuvent être effectuées, à condition que les principes et les obligations du règlement soient respectés. À cet égard, l'introduction d'une hiérarchie implicite entre les architectures technologiques (c'est-à-dire favoriser les grands livres autorisés ou privés par rapport aux grands livres publics et décentralisés) risque de compromettre à la fois le potentiel d'innovation des technologies de la blockchain et la cohérence juridique des lignes directrices elles-mêmes.

En outre, cette position néglige le fait que les blockchains publiques peuvent remplir des fonctions d'importance juridique, sociétale ou économique qui vont au-delà de la protection des données - y compris la transparence, la responsabilité, la prévention de la fraude et le soutien à la gouvernance décentralisée. Limiter leur utilisation au seul motif que l'accès public n'est pas strictement nécessaire à des fins de traitement des données à caractère personnel réduit l'objectif réglementaire et peut entraîner des conséquences imprévues pour l'économie numérique européenne.

Le rôle des autorités chargées de la protection des données ne devrait pas être de déterminer le caractère approprié d'un ensemble technologique donné, mais plutôt d'évaluer si une mise en œuvre donnée est conforme aux principes du GDPR, y compris la minimisation des données, la limitation de la finalité et la sécurité. Une telle approche préserve l'innovation, encourage une conception responsable et garantit que les règles sont appliquées de manière cohérente dans tous les secteurs et toutes les architectures. Les blockchains de la couche 1 publique, en particulier, doivent être considérées comme une infrastructure à usage général, analogue à l'internet lui-même. Elles prennent en charge un large éventail d'applications, de la gestion des identités à la traçabilité de la chaîne d'approvisionnement, et constituent un élément clé de l'écosystème numérique décentralisé émergent. Restreindre leur utilisation par une interprétation étroite risque de pousser l'innovation et le développement d'infrastructures en dehors de l'UE, vers des juridictions dotées de cadres réglementaires plus permissifs ou plus adaptables.

Dans ce contexte, l'Adan invite l'EDPB à réaffirmer son engagement en faveur de la neutralité technologique et à adopter une approche fondée sur des principes et axée sur les risques, qui permette la coexistence de divers modèles architecturaux, à condition que des mesures de protection appropriées soient mises en œuvre.

❖ **Qui est Adan**

L'Adan rassemble plus de 200 professionnels - nouveaux acteurs et entreprises établies - qui développent au quotidien l'innovation et les cas d'usage du web décentralisé dans tous les domaines de l'économie. En levant les obstacles à leur croissance et à leur compétitivité, l'Adan œuvre à l'émergence et au rayonnement de leaders français et européens pour notre souveraineté numérique. L'Adan promeut un cadre adapté, proportionné et dynamique pour l'innovation, ainsi qu'une meilleure compréhension des nouvelles technologies blockchain et Web3 et de leurs opportunités.

❖ **Contacts à l'Adan**

- Stanislas Barthelemi, Président : stanislas.barthelemi@adan.eu
- Adriana Torres Vergara, Chargée de mission UE : adriana.torresvergara@adan.eu
- Alizée Van Den Schrieck, juriste : alizee.vandenschrieck@adan.eu

*