Update Allemagne 2025 – Partie III

Les défis liés à la réglementation croissante

Internet des Objets (IdO): nouvelles règles pour l'accès et l'utilisation des données

Le règlement sur les données modifie fondamentalement le traitement des données. Les entreprises doivent s'adapter à de nouvelles exigences et obligations.

—

RGPD, IA Act, Data Act, etc.: Défis et interfaces réglementaires

La réglementation croissante pose de nouveaux défis aux entreprises. Quelles lois s'imbriquent-elles les unes dans les autres et où surgissent les conflits ?

—

Contrats relatifs à l'exploitation des données: Cadre juridique et bonnes pratiques

Des règles claires en matière de propriété, d'utilisation et de sécurité sont essentielles pour une exploitation efficace des données.

—

Contrôle de conformité : ce que les sociétés doivent désormais respecter dans le traitement des données

Une approche structurée permet d'éviter les risques et d'aligner la stratégie en matière de données sur les exigences légales. Les mesures particulièrement importantes à prendre dès maintenant.

—

Data Act et Intelligence Artificielle

Chères lectrices, chers lecteurs,

La Loi sur les données (Data Act) de l'Union européenne vise à réglementer le marché des données et à établir des règles claires en matière d'utilisation des données.

Parallèlement, l'intelligence artificielle (IA) évolue rapidement et prend une importance croissante dans l'économie et la société. Dans ce domaine également, le législateur européen a posé un cadre juridique de base avec l'entrée en vigueur du règlement sur l'intelligence artificielle (IA Act). Toutefois, ses implications pratiques restent en grande partie floues.

Des questions récurrentes surgissent à propos de ChatGPT, DeepSeek, Mistral & consorts : D'où proviennent les données ? Qu'en est-il de la protection des données personnelles ? Et que dois-je prendre en compte dans ma propre entreprise ?

Avec ce troisième et dernier volet de notre série « Update Allemagne 2025 », nous souhaitons vous informer des dernières évolutions et tenter d'apporter un peu de clarté dans un domaine complexe.

Bonne lecture,

Prof. Dr. Jochen Bauerreis

Update Allemagne 2025 – Partie III

Internet des Objets (IdO): nouvelles règles pour l'accès et l'utilisation des données

Le Data Act de l'Union européenne, entré en vigueur le 11 janvier 2024 et directement applicable dans toute l'UE à partir du 12 septembre 2025, vise à harmoniser l'accès aux données et leur utilisation au sein de l'Union. Il a pour objectif d'améliorer l'utilisation des données dans divers domaines de la vie quotidienne et de contribuer à la création de valeur, notamment au bénéfice de nouveaux modèles économiques, des start-up ainsi que des petites et moyennes entreprises (PME).

Le Data Act comprend une série de dispositions visant à rendre **l'accès aux données et leur utilisation plus équitables et plus transparents**. Cela inclut des règles sur le partage de données entre entreprises et consommateurs (B2C) ainsi qu'entre entreprises (B2B), des obligations pour les détenteurs de données concernant la mise à disposition des données, l'interdiction de clauses contractuelles abusives, ainsi que la mise à disposition de données aux autorités publiques (B2G) en cas d'urgence. En outre, le Data Act définit des exigences contractuelles et techniques pour permettre le changement de prestataire de services de traitement des données (cloud switching).

Un accent particulier est mis sur l'**Internet des objets (« IdO », « Internet of Things » ou « IoT »)**. Les produits IoT (pour simplifier : des produits « connectés ») génèrent une quantité considérable de données, qui sont d'une grande importance tant pour les entreprises que pour les consommateurs. Le Data Act garantit que les utilisateurs de produits IoT ont le droit d'accéder aux données qu'ils génèrent et de les partager avec des tiers. Cela permet un meilleur contrôle sur ses propres données et ouvre de nouvelles opportunités pour les fournisseurs de services, qui peuvent développer des solutions innovantes fondées sur les données. En parallèle, les entreprises doivent veiller à ce que le traitement et le partage de ces données soient conformes aux règles de protection des données personnelles et aux nouvelles exigences réglementaires.

Le Data Act représente une avancée majeure vers un écosystème des données plus équitable et transparent au sein de l'UE. Les entreprises devraient profiter de la période de transition restante pour adapter leurs stratégies en matière de données et prendre les mesures nécessaires afin de se conformer aux nouvelles exigences. En procédant à ces ajustements de manière proactive, elles pourront non seulement garantir leur conformité, mais également tirer parti des nombreuses opportunités offertes par le Data Act. Dans le domaine de l'Internet des objets, en particulier, l'accès facilité aux données permet aux entreprises de développer de nouveaux modèles économiques et d'accélérer leur transformation numérique.

Exemple *:*
Un fabricant d'appareils électroménagers connectés, tels que des réfrigérateurs intelligents ou des thermostats intelligents, pourrait être contraint par le Data Act de donner à ses clients l'accès aux données générées par ces appareils. Jusqu'à présent, ces données étaient principalement utilisées en interne pour améliorer les produits et proposer des services de maintenance. Avec les nouvelles règles, les clients devront cependant être en mesure de transmettre les données de leurs appareils à des prestataires tiers, par exemple, à des fournisseurs d'énergie pour des tarifs d'électricité optimisés ou à des services de réparation indépendants. Cela ouvre de nouvelles perspectives à l'entreprise, notamment à travers des partenariats avec des prestataires de services externes. Cela nécessite toutefois une adaptation des stratégies internes de gestion et de sécurité des données, afin de garantir la protection des données personnelles et de répondre aux exigences réglementaires.

Update Allemagne 2025 – Partie III

RGPD, IA Act, Data Act, etc.: Défis et interfaces réglementaires

La régulation des données et de l'intelligence artificielle (IA) s'intensifie en Europe. Avec le Règlement général sur la protection des données (RGPD), le règlement sur l'intelligence artificielle (IA Act de l'Union européenne) et le Data Act, plusieurs cadres réglementaires sont désormais en place, que les entreprises et organisations doivent prendre en compte dans leurs processus numériques. Mais comment ces textes interagissent-ils, où se trouvent les interfaces, et quels défis en découlent ?

Bien que les différentes bases juridiques régulent des aspects distincts du monde numérique, elles présentent de nombreux points de contact :

- **Utilisation des données et protection des données personnelles** : Le Data Act facilite l'accès aux données non personnelles, mais il doit être mis en cohérence avec le RGPD, afin de garantir qu'aucune donnée à caractère personnel ne soit divulguée de manière illicite.
- **IA et protection des données personnelles :** Les systèmes d'intelligence artificielle reposent souvent sur de grandes quantités de données à caractère personnel, ce qui oblige les entreprises à concilier les exigences du RGPD avec les dispositions du règlement sur l'intelligence artificielle.
- **Responsabilité et conformité :** Les entreprises qui développent ou utilisent des modèles d'intelligence artificielle doivent relever le défi de satisfaire à la fois aux exigences de transparence en matière de règlement sur l'intelligence artificielle et aux obligations en matière de protection des données personnelles imposées par le RGPD.
- **Interopérabilité et accès aux données :** Le Data Act exige une meilleure interopérabilité entre les différents systèmes ainsi qu'une disponibilité accrue des données, ce qui peut entrer en conflit avec les principes prévus par le RGPD en matière de contrôle et de limitation des finalités.

Le respect de plusieurs actes réglementaires qui se chevauchent représente un défi majeur pour les entreprises :

- **Complexité de la mise en œuvre :** Les entreprises doivent veiller à ce que leurs processus numériques soient conformes aux exigences des trois réglementations, ce qui nécessite une stratégie de conformité globale.
- **Pression sur les coûts et mobilisation des ressources :** La mise en œuvre de nouveaux mécanismes de protection des données et de transparence engendre des coûts et requiert une expertise spécialisée.
- **Risques de responsabilité :** Les violations du RGPD, du Data Act ou du règlement sur l'intelligence artificielle peuvent entraîner des sanctions sévères.
- **Défis techniques :** Les exigences en matière de portabilité des données et de transparence nécessitent souvent la mise en place de nouvelles solutions techniques et d'infrastructures informatiques.

L'environnement réglementaire en Europe devient de plus en plus complexe, ce qui représente à la fois un défi et une opportunité pour les entreprises. Si ces lois garantissent la protection des données et des normes éthiques pour les systèmes d'intelligence artificielle, les entreprises doivent fournir des efforts considérables pour répondre aux exigences de conformité. Une gestion de la conformité globale ainsi qu'une adaptation précoce aux obligations réglementaires sont essentielles pour rester compétitif sur le long terme.

Update Allemagne 2025 – Partie III

Contrats relatifs à l'exploitation des données : cadre juridique et bonnes pratiques

La valeur économique des données ne cesse d'augmenter, et les entreprises les utilisent de plus en plus comme une ressource stratégique. Toutefois, pour exploiter les données de manière sécurisée et efficace, des dispositions contractuelles claires sont indispensables. Nous analysons ici les fondements juridiques applicables aux contrats d'exploitation des données et présentons des bonnes pratiques que les entreprises devraient suivre lors de leur élaboration.

Les contrats relatifs à l'exploitation des données sont souvent complexes, car ils évoluent dans un environnement juridique dynamique. Parmi les principaux cadres juridiques à considérer figurent:

- **Droit de la protection des données (RGPD) :** Le traitement des données à caractère personnel est strictement encadré par le Règlement général sur la protection des données (RGPD). Les entreprises doivent s'assurer d'avoir obtenu le consentement des personnes concernées ou de disposer d'une base légale pour le traitement.
- **Droits d'auteur et droits de protection :** Les données peuvent être protégées par le droit d'auteur, le droit des bases de données ou d'autres droits de propriété intellectuelle. Il est alors essentiel de déterminer qui détient les droits sur les données et quels droits d'usage peuvent être cédés.
- **Droit de la concurrence et droit antitrust :** Le partage ou la vente de données entre entreprises peut soulever des problématiques liées au droit de la concurrence. Les règles antitrust doivent être respectées pour éviter tout abus de position dominante ou restriction de concurrence.
- **Droit des contrats :** Les principes du droit des contrats, notamment les clauses relatives à la responsabilité, aux garanties ou aux pénalités contractuelles, sont essentiels pour prévenir les litiges. Il convient également de clarifier la qualification juridique du contrat (vente, location, prestation de services, etc.).

Bonnes pratiques en matière de rédaction contractuelle

Pour élaborer des contrats d'exploitation des données conformes aux exigences juridiques, les entreprises devraient prendre en compte les éléments suivants :

1. ***Définition claire des données**: Le contrat doit préciser quelles données sont concernées, leur origine, ainsi que l'étendue et les modalités de leur utilisation.*
2. ***Droits et obligations des parties contractantes :** Les responsabilités respectives en matière d'utilisation des données doivent être définies sans ambiguïté, notamment en ce qui concerne la protection des données et la sécurité des systèmes.*
3. ***Droits d'usage et limitations:** Le contrat doit indiquer si l'utilisation des données est exclusive ou non exclusive et si des tiers peuvent y accéder.*
4. ***Qualité et sécurité des données :** Des normes relatives à l'intégrité, au chiffrement et au stockage des données doivent être prévues afin de réduire les risques de non-conformité.*
5. ***Durée et résiliation :** Les dispositions relatives à la durée du contrat, aux modalités de résiliation et à la suppression des données à l'issue du contrat doivent être clairement établies.*
6. ***Responsabilité et sanctions :** Le contrat doit préciser les règles de responsabilité en cas de manquement et les sanctions contractuelles applicables en cas de violation des obligations.*

Les contrats relatifs à l'exploitation des données sont un élément essentiel de l'économie moderne fondée sur les données. Les entreprises doivent tenir compte à la fois du cadre juridique applicable et des bonnes pratiques contractuelles afin de minimiser les risques juridiques et de tirer pleinement parti de la valeur des données. Une rédaction contractuelle rigoureuse constitue la clé d'une exploitation des données réussie et juridiquement sécurisée.

Update Allemagne 2025 – Partie III

Contrôle de conformité : ce que les sociétés doivent désormais respecter dans le traitement des données

Les données représentent une ressource précieuse pour les entreprises, mais également un enjeu juridique potentiel. Avec l'accroissement du degré de régulation à travers des textes tels que le Règlement général sur la protection des données (RGPD), le Data Act et le règlement sur l'intelligence artificielle, les exigences en matière de gestion responsable des données se renforcent. Les entreprises doivent s'assurer de respecter l'ensemble des dispositions applicables afin de minimiser les risques juridiques. Un audit de conformité structuré est, dans ce contexte, indispensable.

Les entreprises devraient intégrer les étapes suivantes dans leur audit de conformité :

- √ **État des lieux et inventaire des données** : Les entreprises doivent commencer par un recensement complet des données collectées, traitées et stockées. Cela inclut l'identification des données à caractère personnel et non personnel, ainsi qu'une analyse détaillée des systèmes et processus impliqués dans leur traitement.

- √ **Évaluation des risques et analyse d'impact relative à la protection des données (AIPD)** : Une évaluation approfondie des risques doit être menée afin d'identifier les potentielles violations de données ou failles de sécurité. Pour les traitements sensibles de données personnelles, une analyse d'impact sur la protection des données (AIPD) conformément au RGPD est obligatoire.

- √ **Définir et mettre en œuvre des mesures** : Des mesures techniques et organisationnelles doivent être définies pour assurer la conformité. Cela inclut le chiffrement des données, les contrôles d'accès, les politiques de minimisation des données, ainsi que la formation du personnel.

- √ **Formation et sensibilisation** : La protection des données ne relève pas uniquement du service informatique. Les collaborateurs de tous les services concernés doivent être formés afin de garantir une gestion sécurisée et conforme des données.

- √ **Contrôle régulier et audits** : Les mesures de conformité doivent être revues et actualisées régulièrement. Les entreprises devraient réaliser des audits internes périodiques pour vérifier le respect des obligations légales en vigueur et identifier les failles potentielles.

- √ **Clarification des responsabilités** : Il est essentiel de déterminer qui, au sein de l'entreprise, est responsable du respect des différentes exigences réglementaires. Les délégués à la protection des données ou les responsables « conformité » (compliance) jouent ici un rôle central dans la mise en œuvre et le suivi des mesures.

- √ **Gestion des incidents et stratégies de réaction** : Les entreprises doivent disposer de processus clairs pour faire face aux violations de données et aux incidents de sécurité. Cela inclut un système de notification efficace, ainsi qu'un plan de communication à l'attention des utilisateurs concernés et des autorités de contrôle.

Vous avez des questions ? Nous nous tenons bien entendu à votre disposition pour toute information complémentaire sur les sujets susmentionnés ou pour toute demande de conseil individuel.

Notre cabinet d'avocats international ABCI ALISTER, implanté à Strasbourg & Kehl ainsi qu'à Paris, Lyon, Nice, Montpellier et Montélimar, conseille les entreprises dans tous les domaines du droit international des affaires, allemand et français.

Sur les sites de Strasbourg & Kehl, nous disposons d'une équipe multilingue d'une dizaine de personnes composée d'avocats et de Rechtsanwälte inscrits au(x) barreau(x) allemand et/ou français.

Les principaux domaines de notre conseil juridique et stratégique sont les suivants :

- ***Mergers & Acquisitions (M & A)***
- ***Corporate***
- ***Human Ressources***
- ***Compliance***
- ***International***
- ***Restructuring***
- ***Services & Products***
- ***Litigation***