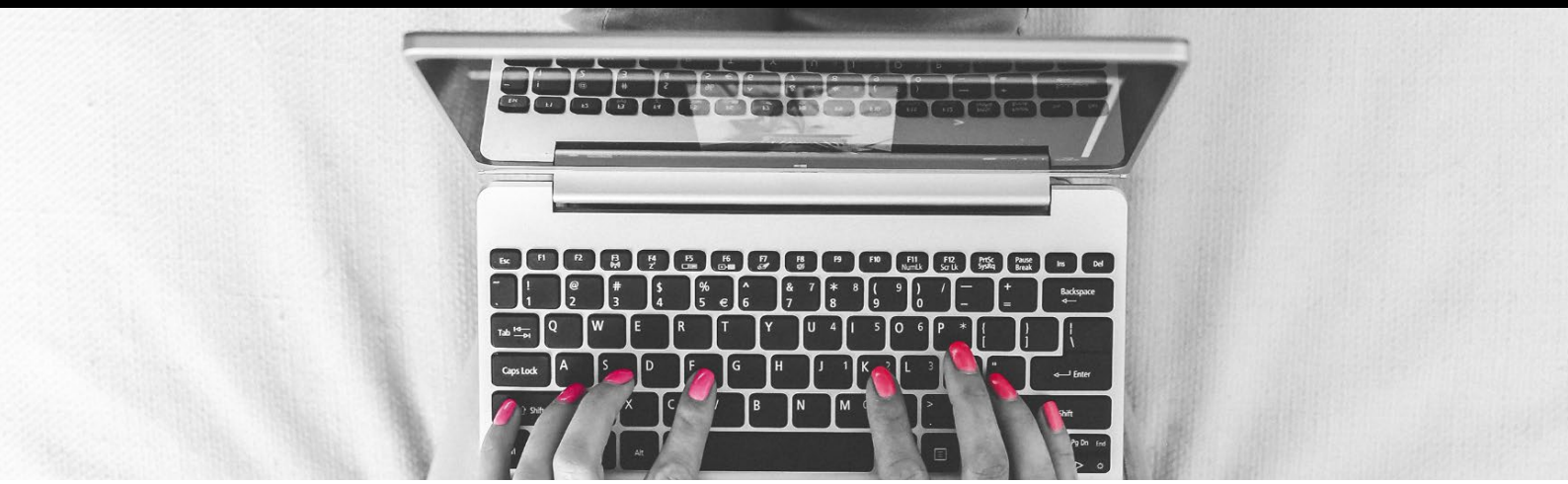
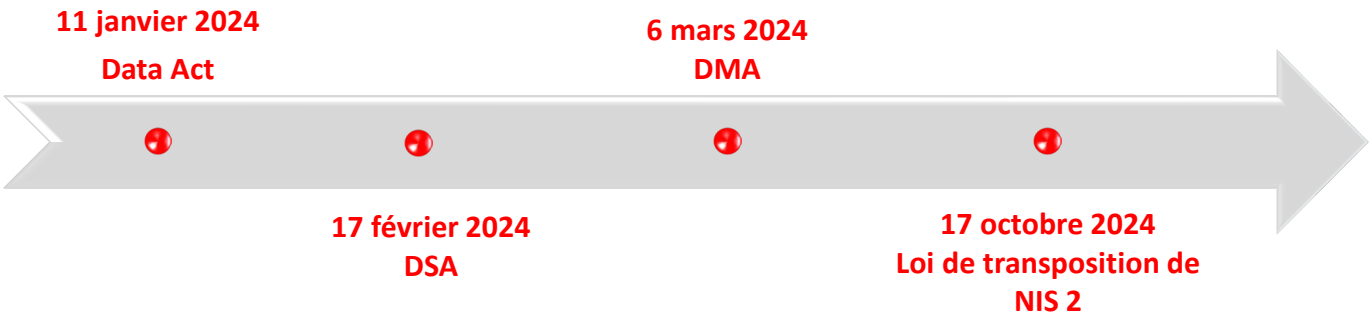
2024 : Quelles sont les nouvelles obligations pesant sur les entreprises dans le secteur du numérique ?

J&A



En 2024, les entreprises évoluant dans le secteur du numérique seront soumises à de nouvelles obligations réglementaires qu'il vient d'anticiper dès à présent.

Tour d'horizon des nouvelles règles à venir.



1) Data Act : entrée en vigueur au 11 janvier 2024

Le règlement (UE) 2023/2854 du 13 décembre 2023 concernant des règles harmonisées portant sur l'équité de l'accès aux données et de l'utilisation des données (« **Règlement sur les données** » ou « **Data Act** ») est entré en vigueur **le 11 janvier 2024 et sera applicable dans tous les Etats Membres à compter du 12 septembre 2025**.

Le Data Act a vocation à garantir l'équité dans la répartition de la valeur produite par les données entre les entreprises, les utilisateurs et les autorités publiques dans l'objectif de créer un marché unique de la donnée.

Le Data Act concerne tant les données personnelles que les données non-personnelles (données industrielles brutes, données relatives à la performance, à l'utilisation et à l'environnement des produits connectés, données traitées par des fournisseurs de services de traitement de données…).

Ce règlement concerne plus particulièrement les fabricants de produits et de services connectés et les fournisseurs de services de traitement de données (services de « cloud ») qui proposent des produits et services sur le marché de l'Union, indépendamment de leur lieu d'établissement.

Un service de traitement est défini comme un « *service numérique qui est fourni à un client et qui permet un accès par réseau en tout lieu et à la demande à un ensemble partagé de ressources informatiques configurables, modulables et variables de nature centralisée, distribuée ou fortement distribuée, qui peuvent être rapidement mobilisées et libérées avec un minimum d'efforts de gestion ou d'interaction avec le fournisseur de services* ».

Parmi les mesures phares du règlement, figurent :

- L'obligation pour les fournisseurs de mettre à disposition des utilisateurs (consommateur ou professionnel) et/ou dans certains cas aux autorités publiques, les données générées par ces produits [4]. Ces données doivent être accessibles sans retard excessif, gratuitement et en permanence.
- Le droit pour l'utilisateur d'obtenir la portabilité des données vers un tiers offrant le même type de services que ceux de l'entité lui ayant vendu ou loué originellement le bien ou le service.
- Le Data Act liste les clauses présumées abusives dans les contrats de partage des données imposées unilatéralement par une entreprise[6]. La commission va élaborer des clauses contractuelles types afin d'aider les acteurs à rédiger des contrats équitables.
- Les exigences essentielles auxquelles doivent répondre les «*smart contracts*» créés par les développeurs professionnels et intégrés dans des applications ;
- La sécurisation des transferts internationaux de données et notamment la nécessité de de prendre « *toutes les mesures techniques, juridiques et organisationnelles raisonnables* » afin d'empêcher le transfert hors du territoire européen de données ou l'accès d'États tiers à celles-ci.

Le Data Act supprime également les obstacles au changement de service de traitement des données[9]. **L'article 29 du Data Act prévoit une suppression progressive des frais de changement de fournisseur à la charge du client, dès le 11 janvier 2024.**

Il dispose en effet que :

> *« 1. À compter du 12 janvier 2027, les fournisseurs de services de traitement de données **ne peuvent imposer aucun frais de changement de fournisseur** au client pour le processus de changement de fournisseur*
>
> *2. **À compter du 11 janvier 2024 et jusqu'au 12 janvier 2027**, les fournisseurs de services de traitement de données **peuvent** imposer des frais de changement de fournisseur réduits au client, pour le processus de changement de fournisseur.*
>
> *3. Les frais de changement de fournisseur réduits visés au paragraphe 2 ne dépassent pas les coûts supportés par le fournisseur de services de traitement de données qui sont directement liés au processus de changement de fournisseur concerné. »*

Ainsi, depuis le 11 janvier 2024 et jusqu'au 12 janvier 2027, les fournisseurs de service pourront imposer des frais de changement réduits à leur client, ces derniers ne devront pas dépasser les couts supportés par le fournisseur lui-même. En tout état de cause, aucun frais de changement de fournisseur ne pourra être demandé à compter du 12 janvier 2027.

A noter : les Etats Membres devront déterminer le régime des sanctions au plus tard le 12 septembre 2025. Ainsi, les sanctions ne seront applicables qu'à compter de cette date.

Les actions à prendre d'ici 2025 sont *a minima* les suivantes :

- **Revoir ses conditions contractuelles pour identifier les éventuelles clauses abusives portant atteinte de manière injustifiée aux droits des utilisateurs ;**
- **Informer les clients sur les modalités d'accès aux données, de changement de fournisseur et les étapes du processus de migration ainsi que ses effets le cas échéant, dans les conditions générales de vente ou une rubrique dédiée.**

2) DSA : 17 février 2024

Le règlement du Parlement européen et du conseil n°2022/2065 du 19 octobre 2022 (« **Digital Service Act** » ou « **DSA »**) fixe un ensemble de règles visant à responsabiliser les intermédiaires en ligne (tels que les fournisseurs d'accès internet, services cloud, marketplaces, réseaux sociaux) fournissant des services ou des produits à des destinataires situés au sein de l'Union européenne.

Ces plateformes ont **jusqu'au 17 février 2024** pour se mettre en conformité, étant précisé que les très grandes plateformes en ligne et les très grands moteurs de recherche doivent déjà respecter ces obligations depuis le 25 août 2023.

Le DSA vise à (i) encadrer la relation entre les plateformes et les consommateurs et (ii) protéger les droits fondamentaux des internautes garantis par la Charte des droits fondamentaux de l'Union européenne. Pour ce faire, le DSA impose de nouvelles obligations aux opérateurs numériques en matière de légalité des contenus et de transparence des algorithmes de recommandation et de publicité. L'objectif est également de lutter contre la désinformation en ligne.

Le DSA a un champ d'application très large et impose des obligations différentes selon la taille de l'intermédiaire concerné et la nature du service rendu.

En cas de non-respect du DSA, les sanctions sont les suivantes :

- Une amende pouvant aller jusqu'à 6% de son chiffre d'affaires mondial total,
- Une mesure temporaire de restriction de l'accès au service.

Les destinataires des services peuvent en outre demander réparation aux prestataires pour les dommages ou pertes subis en raison d'une violation des dispositions du DSA.

<table>
<tr><th colspan="3">Le DSA impose en particulier :</th></tr>
<tr><td rowspan="3">à tous les fournisseurs de services intermédiaires</td><td colspan="2">- désigner et publier un point de contact et un représentant légal, le cas échéant ;
- mettre à jour les conditions générales de vente avec les informations relatives aux procédures internes mises en place pour lutter contre les contenus illicites ;
- publier un rapport annuel de transparence sur les éventuelles activités de modération des contenus au cours de la période concernée.</td></tr>
<tr><td>aux services d'hébergement</td><td>- mettre en œuvre des mécanismes d'information de la présence de contenus présumés illicites ;
- exposer à l'utilisateur concerné par la procédure de retrait les motifs de ce retrait (comprenant les faits fondant la décision, les informations sur l'utilisation de moyens automatisés, le motif légal ou contractuel, les voies de recours) ;
- informer les autorités répressives ou judiciaires nationales de l'État membre concernées de toute information donnant lieu à des soupçons d'infractions pénales impliquant une menace pour la vie ou la sécurité des personnes.</td></tr>
<tr><td>aux places de marché

(sauf celles considérées comme des micro-entreprises et petites entreprises)</td><td>- effectuer des contrôles KYBC sur les nouveaux professionnels qui proposent des produits ou des services aux consommateurs dans l'UE par leur intermédiaire, en s'assurant que les informations fournies sont fiables et complètes ;
- veiller à ce que leurs interfaces permettent le respect des informations précontractuelles, de conformité et des informations relatives à la sécurité des produits ;
- informer les consommateurs concernés lorsque l'un des professionnels proposent un produit ou service illégal par leur intermédiaire.</td></tr>
</table>

			- mettre en place un système de traitement des plaintes contre une décision de suppression, de désactivation, de suspension ou de résiliation de l'accès d'un utilisateur à des informations, à des services ou à son compte ; - informer les plaignants de sa décision et des options pour un règlement à l'amiable ou d'autres voies de recours ; - donner la priorité aux avis de signaleurs de confiance ; - suspendre, pendant une période raisonnable et après avoir émis un avertissement préalable, la fourniture de services aux destinataires du service qui fournissent fréquemment des contenus manifestement illicites ; - suspendre le traitement des notifications abusives des plaignants qui soumettent des notifications infondées ; - intégrer aux rapports de transparence des informations (nombre de litiges transmis aux organes de règlement extrajudiciaire, délai médian pour mener à bien les procédures de règlement de litige, nombre de suspension imposé) ; - publier des informations sur les destinataires actifs mensuels moyens du service ; - veiller à ce que les interfaces en ligne ne soient pas de nature à tromper ou à manipuler les destinataires du service ou propres à altérer ou à entraver substantiellement la capacité des destinataires du service à prendre des décisions libres et éclairées ; - informer clairement les utilisateurs du caractère publicitaire des publications sur la plateforme et fournir les informations relatives à cette publicité ; - ne pas présenter des publicités ciblées basées sur le profilage en utilisant les données personnelles des mineurs ou des données sensibles ; - s'ils utilisent des systèmes de recommandation, indiquer les principaux paramètres utilisés dans les systèmes de recommandation et les options pour modifier ou influencer ces principaux paramètres.
		aux fournisseurs de très grandes plateformes en ligne et de très grands moteurs de recherche en ligne	- évaluer annuellement des risques systémiques découlant du fonctionnement et de l'utilisation de leurs services et atténuer les risques identifiés ; - mettre en place une fonction de conformité indépendante des fonctions opérationnelles ; - à la demande de la Commission, évaluer si leurs services contribuent à une menace grave, identifier des mesures pour éliminer cette contribution et faire un rapport sur ces évaluations ; - se soumettre à des audits annuels indépendants ; - donner accès aux données nécessaires au contrôle à la demande du coordinateur des services numériques ; - publier un registre d'informations sur les publicités diffusées ; - Intégrer aux rapports de transparence des informations (informations sur les ressources humaines affectées à la modération du contenu).

3) DMA : 6 mars 2024

Le règlement du Parlement européen et du conseil n°2022/1925 du 14 septembre 2022 relatif aux marchés contestables et équitables dans le secteur numérique (« **Digital Market Act** » ou « **DMA** ») est entré en application le 2 mai 2023.

Il encadre les activités économiques des plus grandes plateformes (les « **contrôleurs d'accès** »).

Un contrôleur d'accès est une plateforme qui :

- a un poids important sur le marché intérieur (en réalisant au moins 7,5 milliards d'euros de chiffre d'affaires dans l'Espace économique européen au cours de chacun des trois derniers exercices ou si sa capitalisation boursière ou sa valeur marchande a atteint au moins 75 milliards d'euros au cours du dernier exercice, avec une activité dans au moins trois Etats membres) ;
- fournit un service de plateforme essentiel qui constitue un point d'accès majeur permettant aux entreprises utilisatrices d'atteindre leurs utilisateurs finaux (en fournissant un service de plateforme essentiel qui, au cours du dernier exercice, a compté au moins 45 millions d'utilisateurs finaux actifs par mois établis ou situés dans l'Union et au moins 10 000 entreprises utilisatrices actives par an établies dans l'Union) ; et
- jouit d'une position solide et durable, dans ses activités, ou jouira, selon toute probabilité, d'une telle position dans un avenir proche.

Le législateur européen entend lutter contre les positions dominantes des contrôleurs d'accès. Ces derniers ne peuvent notamment pas :

- favoriser leurs propres services et produits par rapport à ceux des entreprises qui les utilisent ;
- exploiter les données des entreprises qui utilisent leurs services pour les concurrencer ;
- imposer des logiciels par défaut à l'installation de leur système d'exploitation.

Les principaux services de messagerie (Whatsapp, Facebook Messenger, iMessage…) doivent être interopérables avec leurs concurrents.

Enfin, les contrôleurs d'accès devront informer la Commission des acquisitions et fusions qu'ils réalisent.

- **Les contrôleurs d'accès ont jusqu'au 6 mars 2024 maximum pour démontrer à la Commission européenne qu'ils respectent bien leurs obligations.**

4) NIS 2 – cybersécurité : 17 octobre 2024

La directive du Parlement européen et du conseil n°2022/2555 du 14 décembre 2022 (« **Network and Information Security** » ou **« NIS 2** ») a pour objectif de remplacer la directive n°2016/1148 relative à la cybersécurité.

Chaque Etat membre dispose d'un délai de 21 mois pour transposer en droit national les différentes exigences réglementaires. NIS 2 devra donc être transposée en droit français au plus tard le 17 octobre 2024. NIS sera abrogée le 18 octobre 2024.

NIS 2 a une application plus large que NIS dans la mesure où elle cible un nombre d'acteurs économiques plus importants, qu'ils appartiennent au secteur public ou privé. L'adoption de NIS 2 représente le passage d'une « cybersécurité des opérateurs critiques » à une « cybersécurité de masse ».

1. Etes-vous concernés ?

Sont concernées par NIS 2 :

- les entités privées ou publiques d'un type visé à l'annexe 1 ou 2, (ii) qui constituent des entreprises moyennes (ayant plus de 50 employés et un chiffre d'affaires annuel ou le total du bilan annuel est supérieur à 10 millions d'euros) et (iii) qui fournissent leurs services ou exercent leurs activités au sein de l'Union européenne.
- les entités d'un type visé à l'annexe 1 ou 2, quelle que soit leur taille lorsqu'elles sont notamment essentielles au fonctionnement de l'Etat ;
- les entités étant recensées par les Etats membres comme critiques, visées par la directive n°2022/2557 du 14 décembre 2022, quelle que soit leur taille ;
- les entités fournissant des services d'enregistrement de noms de domaine quelle que soit leur taille.

Les secteurs « hautement critiques » visés à l'annexe 1 de NIS 2 sont les suivants :

- Energie
- Transport
- Secteur bancaire
- Infrastructure des marchés financiers
- Santé
- Infrastructure numérique (prestataires de services de confiance, fournisseur de services cloud, fournisseurs de services DNS, fournisseurs de réseaux de diffusion de contenu, fournisseurs de services de centre de données, fournisseurs de services de communications électroniques accessibles au public…)
- Eau potable
- Eaux usées
- Espace
- Gestion des services TIC
- Administration publique

Les autres secteurs critiques, visés à l'annexe 2 de NIS 2, sont les suivants :

- Services postaux et d'expédition
- Gestion des déchets
- Fabrication, production et distribution de produits chimiques
- Production, transportation et distribution des denrées alimentaires
- Fabrication (dispositif médicaux, produits informatiques, matériels de transport…)
- Fournisseurs numériques (marketplaces, moteurs de recherche, services de réseaux sociaux)

2. Quelles sont les obligations prévues par NIS 2 ?

NIS 2 crée deux nouvelles typologies d'entreprises selon leur niveau de criticité :

- **les entités essentielles (EE)** : ce sont notamment – mais pas exclusivement – celles réalisant des activités dans les secteurs catégorisés comme hautement critiques et disposant de plus de 250 salariés et dont le chiffre d'affaires annuel est supérieur à 50 millions d'euros ;

- **les entités importantes (EI) :** elles sont définies par la négative dans la mesure où elles regroupent les entités qui ne sont pas des EE au sens de NIS 2.

Les Etats membres ont jusqu'au 17 avril 2025 pour recenser les EE et les EI.

Les EE et les EI devront :

- prendre des **mesures techniques, opérationnelles et organisationnelles appropriées et proportionnées** pour gérer les risques qui menacent la sécurité des réseaux et des systèmes d'information qu'elles utilisent dans le cadre de leurs activités ou de la fourniture de leurs services, ainsi que pour éliminer ou réduire les conséquences que les incidents ont sur les destinataires de leurs services.

  Les mesures sont fondées sur une approche « tous risques » et comprennent au moins :

  - les politiques relatives à l'analyse des risques et à la sécurité des systèmes d'information ;
  - la gestion des incidents ;
  - la continuité des activités, par exemple la gestion des sauvegardes et la reprise des activités, et la gestion des crises ;
  - la sécurité de la chaîne d'approvisionnement, y compris les aspects liés à la sécurité concernant les relations entre chaque entité et ses fournisseurs ou prestataires de services directs ;
  - la sécurité de l'acquisition, du développement et de la maintenance des réseaux et des systèmes d'information, y compris le traitement et la divulgation des vulnérabilités ;
  - des politiques et des procédures pour évaluer l'efficacité des mesures de gestion des risques en matière de cybersécurité ;
  - les pratiques de base en matière de cyber-hygiène et la formation à la cybersécurité ;
  - des politiques et des procédures relatives à l'utilisation de la cryptographie et, le cas échéant, du chiffrement ;
  - la sécurité des ressources humaines, des politiques de contrôle d'accès et la gestion des actifs ;
  - l'utilisation de solutions d'authentification à plusieurs facteurs ou d'authentification continue, de communications vocales, vidéo et textuelles sécurisées et de systèmes sécurisés de communication d'urgence au sein de l'entité, selon les besoins.

Lorsqu'une entité constate qu'elle ne se conforme pas aux mesures prévues, elle doit prendre, sans retard injustifié, toutes les mesures correctives nécessaires appropriées et proportionnées.

Au plus tard le 17 octobre 2024, la Commission adoptera des actes d'exécution établissant les exigences techniques et méthodologiques liées aux mesures visées ci-dessus en ce qui concerne un certain nombre d'entités.

- notifier, sans retard injustifié, au centre de réponse aux incidents informatiques (« CSIRT ») ou, selon le cas, à son autorité compétente, tout incident ayant un impact important sur leur fourniture des services. Le cas échéant, les entités concernées notifient, sans retard injustifié, aux destinataires de leurs services les incidents importants susceptibles de nuire à la fourniture de ces services.

3. Quelles sont les sanctions prévues par NIS 2 ?

L'ANSSI aura la capacité de réaliser des contrôles pouvant conduire à des injonctions en cas de non-conformité identifiée. Dans ce cadre, l'agence travaille actuellement à la définition des mécanismes de contrôle qui seront adaptés au passage à l'échelle que représente NIS 2.

Des sanctions administratives pourront être infligées aux EE et EI qui violent les dispositions de NIS 2.

- Pour les EE : Un montant minimum de 10 millions d'euros ou à 2% du chiffre d'affaires ; et
- Pour les EI un minimum de 7 millions d'euros ou 1,4% du chiffre d'affaires.

Il conviendra d'attendre la transposition de la directive en droit interne pour en savoir plus.

Notre équipe IT/Data se tient à votre disposition pour toutes questions

Emilie de VAUCRESSON
Avocate associée
edevaucresson@joffeassocies.com

Amanda DUBARRY
Avocate
adubarry@joffeassocies.com

Camille LEFLOUR
Avocate
cleflour@joffeassocies.com