Le contenu de ce document est protégé par le secret professionnel
article 226-13 du Code pénal

LEGAL OPINION / consultation juridique

Diagnostic positionnement législation cyber-sécurité

NIS2 + ReX NIS2 + REC + DORA

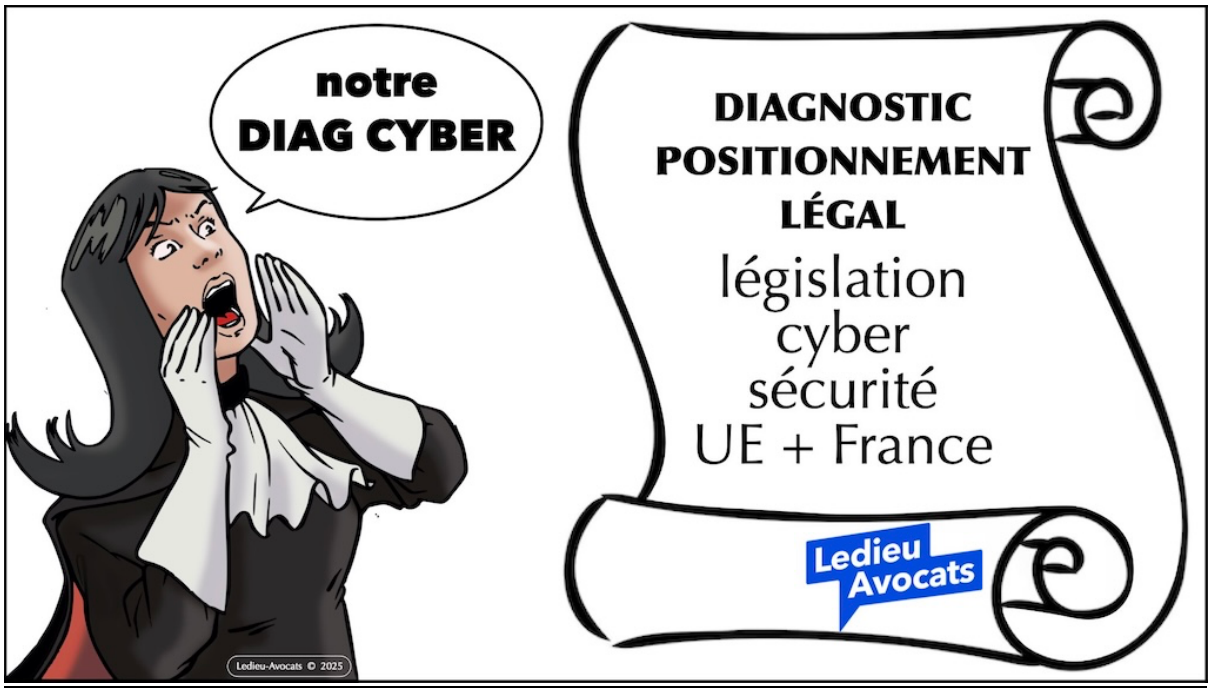
EXEMPLE FICTIF POUR INFORMATION

Paris, le 16 septembre 2026

DESTINATAIRE(S) : [société/groupe CLIENT]

DIFFUSION : **<u>besoin d'en connaitre</u> - INTERNE** [société/groupe CLIENT] **seulement**

TRANSMISSION : Ce document est transmissible à toute autorité de contrôle (ANSSI, etc.) et peut être produit en justice comme preuve écrite des diligences accomplies par [société/groupe CLIENT] dans son process de déploiement des obligations légales imposées par la Directive NIS2 / le Règlement DORA.



01 (legal opinion) NOS CONCLUSIONS sur le positionnement cyber-sécurité NIS2 / ReX NIS2 / DORA de [société/groupe CLIENT]

01.01 Eléments légaux pris en compte

01.01.1 Ledieu-Avocats a analysé les éléments transmis par [société/groupe CLIENT] (notre "QUESTIONNAIRE : les données légales").

01.02 RAPPEL des textes légaux pris en compte

01.02.1 Ledieu-Avocats a pris en compte avec [société/groupe CLIENT] les secteurs régulés par (voir la liste exhaustive au paragraphe "NIS2 - Textes légaux de référence"):

(i) la Directive UE n°2022/2555 du 14 décembre 2022 ;

(ii) le Règlement d'exécution UE "entités et réseaux critiques" n°2024/2690 du 17 octobre 2026 ;

(iii) le Règlement UE "DORA" n°2022/2554 du 14 décembre 2022 ;

(iv) la Directive UE "Résilience des entités critiques" dite REC n°2022/2557 du 14 décembre 2022 :

(v) le projet de loi "Résilience des infrastructures critiques" dans sa dernière version publique ;

(vi) le projet de décret public de l'ANSSI publié le 17 mars 2026 (projet "RéCyF v2.5).

01.02.2 Les conclusions provisoires de Ledieu-Avocats ont fait l'objet d'une validation écrite par [société/groupe CLIENT] (voir "Méthodologie et versioning).

01.02.3 Ledieu-Avocats est en mesure de confirmer officiellement le diagnostic "positionnement légal NIS2 / ReX NIS2 / REC / DORA" de [société/groupe CLIENT] comme suit.

01.03 Les conclusions de Ledieu-Avocats

01.03.1 **Conclusion NIS2 Annexe 1 secteur #01 ENERGIE : l'activité de [société/groupe CLIENT] est soumise à la Directive NIS2 n°2022/2555 du 14 décembre 2022.**

(i) **Secteur NIS2 de référence** : #NIS2#Annexe 1 [hautement critique]#1#a# ENERGIE / "**entreprises d'électricité**" au sens de l'article 2.57) de la directive (UE) 2019/944 "**qui assure la fonction de fourniture" [d'électricité]** au sens de l'article 2.12) de la directive (UE) 2019/944.

01.03.2 L'activité de [société/groupe CLIENT] n'est pas soumise au Règlement d'exécution [entités et réseaux critiques] n°2024/2690 du 17 octobre 2024.

01.03.3 L'activité de [société/groupe CLIENT] n'est pas soumise au Règlement DORA n°2022/2554 du 14 décembre 2022.

01.03.4 A la date de rédaction du présent document, [société/groupe CLIENT] est "**entité importante**" #EI :

(i) Nombre total de salariés ETP [[société/groupe CLIENT] date] : _____ ETP

(ii) Cumul CA / bilan [société/groupe CLIENT] : _____ € HT

01.04 Conséquences pour [société/groupe CLIENT]

01.04.1 En qualité d'**entité importante**, [société/groupe CLIENT] est tenu de se déclarer comme tel à l'ANSSI via le portail en ligne (version béta) :

01.04.2 [société/groupe CLIENT] est tenu de mettre en œuvre - de manière effective et auditable - les mesures fixées dans le PROJET de decret "RéCyF" du 17 mars 2026 qui s'imposent aux **entités importantes** #EI (**SANS analyse des risques préalable**) :

#01) Recensement des systèmes d'information #EI+EE#

#02) Mise en oeuvre d'un cadre de gouvernance de la sécurité numérique #EI+EE#

#03) Maîtrise de l'écosystème #EI+EE#

#04) Intégration de la sécurité numérique dans la gestion des RH #EI+EE#

#05) Maîtrise des systèmes d'information #EI+EE#

#06) Maîtrise des accès physiques aux locaux #EI+EE#

#07) Sécurisation de l'architecture des systèmes d'information #EI+EE#

#08) Sécurisation des accès distants aux systèmes d'information #EI+EE#

#09) Protection des systèmes d'information contre les codes malveillants #EI+EE#

#10) Gestion des identités et des accès des utilisateurs aux SI #EI+EE#

#11) Maîtrise de l'administration des systèmes d'information #EI+EE#

#12) Identification et réaction aux incidents de sécurité #EI+EE#

#13) Continuité et reprise d'activité #EI+EE#

#14) Réaction aux crises d'origine cyber #EI+EE#

#15) Exercices, tests et entrainements #EI+EE#

01.05 NIS2 - Conséquences pour entité importante : liste des documents juridiques à rédiger

(i)

(ii)

(iii)

(iv)

01.06 NIS2 - recommandation de process à mettre en oeuvre par [société/groupe CLIENT]

(i)

(ii)

(iii)

(iv)

01.07 NIS2 entité importante : RAPPEL du risque de sanction pour [société/groupe CLIENT]

01.07.1 Amende administrative pour [société/groupe CLIENT] : jusqu'à **SEPT (7) millions euros** ou **UN virgule QUATRE (1,4) %** du chiffre d'affaires annuel mondial total #NIS2#34#5#

01.08 NIS2 entité importante : RAPPEL des pouvoirs de contrôle de l'ANSSI #NIS2#33.2#

"a) des inspections sur place et des contrôles à distance ex post, effectués par des professionnels formés;

b) des audits de sécurité ciblés réalisés par un organisme indépendant ou une autorité compétente;

c) des scans de sécurité fondés sur des critères d'évaluation des risques objectifs, non discriminatoires, équitables et transparents, si nécessaire avec la coopération de l'entité concernée;

d) des demandes d'informations nécessaires à l'évaluation ex post des mesures de gestion des risques en matière de cybersécurité adoptées par l'entité concernée, notamment les politiques de cybersécurité consignées par écrit, ainsi que du respect de l'obligation de soumettre des informations aux autorités compétentes conformément à l'article 27;

e) des demandes d'accès à des données, à des documents et à des informations nécessaires à l'accomplissement de leurs tâches de supervision;

f) des demandes de preuves de la mise en œuvre de politiques de cybersécurité, telles que les résultats des audits de sécurité effectués par un auditeur qualifié et les éléments de preuve sous-jacents correspondants."

01.09 NIS2 entité importante : RAPPEL des pouvoirs de sanction de l'ANSSI #NIS2#33.4#

a) émettre des avertissements concernant des violations de la présente directive par les entités concernées;

b) adopter des instructions contraignantes ou une injonction exigeant des entités concernées qu'elles pallient les insuffisances constatées ou les violations de la présente directive;

c) ordonner aux entités concernées de mettre un terme à un comportement qui viole la présente directive et de ne pas le réitérer;

d) ordonner aux entités concernées de garantir la conformité de leurs mesures de gestion des risques en matière de cybersécurité avec l'article 21 ou de respecter les obligations d'information prévues à l'article 23, de manière spécifique et dans un délai déterminé;

e) ordonner aux entités concernées d'informer les personnes physiques ou morales à l'égard desquelles elles fournissent des services ou exercent des activités susceptibles d'être affectées par une cybermenace importante de la nature de la menace, ainsi que de toutes mesures préventives ou réparatrices que ces personnes physiques ou morales pourraient prendre en réponse à cette menace;

f) ordonner aux entités concernées de mettre en œuvre les recommandations formulées à la suite d'un audit de sécurité dans un délai raisonnable;

g) ordonner aux entités concernées de rendre publics des aspects de violations de la présente directive de manière spécifique;

h) d'imposer ou de demander aux organes compétents ou aux juridictions compétentes d'imposer, conformément au droit national, une amende administrative en vertu de l'article 34 en plus de l'une ou l'autre des mesures visées aux points a) à g) du présent paragraphe.

01.10 NIS2 entité importante : proposition d'accompagnement par Ledieu-Avocats

01.10.1 Ledieu Avocats est en mesure d'accompagner [société/groupe CLIENT] dans sa compréhension et sa sensibilisation aux impératifs (i) gouvernance, (ii) techniques et (iii) juridiques de la Directive NIS2 et de sa transposition en droit français.

01.10.2 Ledieu Avocats est également en mesure d'accompagner [société/groupe CLIENT] dans dans la rédaction de l'ensemble de ses documents juridiques indispensables à sa mise en conformité à la législation NIS2, tant vis-à-vis de ses clients utilisateurs finaux que vis-à-vis de ses prestataires sous-traitants et développeurs logiciel.

sommaire détaillé
du DIAG CYBER positionnement NIS2 / ReX NIS2 / REC / DORA