silex | PROTECTION DES DONNÉES ET CYBERSÉCURITÉ

Guide sur la Directive NIS2

Présentation complète

Mars 2025

Table des matières

Objectif

La directive NIS 2 a pour but de **renforcer la cyberrésilience** au sein de l'Union Européenne. Elle s'inscrit dans une démarche visant à moderniser l'approche réglementaire de la cybersécurité, en réponse aux lacunes identifiées dans la directive NIS précédente.

Elle vise à assurer la **continuité des services essentiels** en cas d'incidents, contribuant ainsi à la sécurité de l'UE et au bon fonctionnement de son économie et de sa société.

Un des objectifs clés est d'**éliminer la distinction** obsolète entre les opérateurs de services essentiels et les fournisseurs de services numériques, en reconnaissant l'importance réelle de chaque secteur et service pour le marché intérieur.

La directive prévoit la mise en place de **stratégies nationales de cybersécurité** et la désignation d'autorités compétentes pour superviser et appliquer les mesures de cybersécurité.

Champ d'application

La directive s'applique aux entités considérées comme **essentielles** ou **importantes** selon les annexes I et II, en fonction de leur taille et de leur rôle dans l'économie.

Elle s'étend à une **partie plus large de l'économie**, couvrant des secteurs et services vitaux pour les activités sociales et économiques du marché intérieur.

Les secteurs inclus dans les annexes I et II comprennent :

- Énergie
- Transports
- Secteur bancaire
- Infrastructures des marchés financiers
- Santé
- Eau potable
- Eaux usées
- Infrastructure numérique
- Gestion des services TIC
- Administration publique
- Espace
- Services postaux et d’expédition
- Gestion des déchets
- Fabrication, production et distribution de produits chimiques
- Production, transformation et distribution de denrées alimentaires
- Fabrication
- Fournisseurs numériques
- Recherche

Les États membres doivent établir une **liste des entités essentielles et importantes**. Ils peuvent également mettre en place des mécanismes nationaux pour permettre aux entités de s'enregistrer.

La directive ne s'applique pas aux entités exerçant des activités dans les domaines de la sécurité nationale, de la défense ou de l'application de la loi.

Principales obligations

Mesures de gestion des risques (sécurité des systèmes d'information)

Les entités essentielles et importantes doivent adopter des **mesures techniques, opérationnelles et organisationnelles appropriées** pour gérer les risques pesant sur la sécurité de leurs réseaux et systèmes d'information. Ces mesures de sécurité doivent être proportionnées aux risques encourus, à la taille de l'entité, ainsi qu'à la probabilité et à l'impact potentiel des incidents.

L'article 21 de la directive précise que l'approche doit être globale (« approche tous risques ») et couvre *au minimum* les domaines suivants : **politique de gestion des risques et de sécurité des systèmes d'information**, **gestion des incidents**, **plan de continuité des activités** (sauvegardes, reprise après sinistre, gestion de crise), **sécurité de la chaîne d'approvisionnement**, **sécurité dans l'acquisition, le développement et la maintenance des SI** (y compris gestion des vulnérabilités), **évaluation de l'efficacité des mesures** mises en place, **pratiques de cyber-hygiène et formation du personnel**, **politiques d'utilisation de la cryptographie** (ex : chiffrement approprié), **sécurité des ressources humaines et contrôle d'accès**, et **authentification multi-facteurs et communications d'urgence sécurisées**.

Ces obligations incitent donc les entités à mettre en place un véritable **système de management de la sécurité de l'information (SMSI)** interne, couvrant tant la prévention (analyse des risques, mesures de protection) que la réaction aux incidents et la résilience.

Sécurité de la chaîne d'approvisionnement

Une nouveauté importante de NIS 2 est l'accent mis sur la **gestion des risques liés aux fournisseurs et prestataires**. Les entités doivent intégrer, parmi leurs mesures de sécurité, des politiques de **sécurité des relations avec les fournisseurs** et tenir compte des vulnérabilités propres à chacun de leurs prestataires critiques. La directive souligne que les attaques provenant de failles chez les tiers (fournisseurs de logiciels, sous-traitants techniques, etc.) peuvent compromettre gravement une entité essentielle.

Il est donc attendu des entités qu'elles évaluent la **fiabilité et la résilience des produits et services tiers** qu'elles utilisent, et qu'elles encouragent l'intégration de clauses de cybersécurité dans les contrats avec leurs fournisseurs. Par ailleurs, la Commission pourra adopter des actes d'exécution pour préciser les exigences de sécurité applicables à certaines catégories d'entités sur des aspects particuliers, afin d'assurer une harmonisation (par exemple, critères pour qu'un incident soit qualifié de « critique » dans tel secteur).

Les États membres, de leur côté, peuvent **encourager ou exiger** l'usage de produits et services certifiés en cybersécurité : NIS 2 prévoit en effet la possibilité d'imposer le recours à des solutions certifiées selon des schémas européens (conformément au règlement (UE) 2019/881 – Cybersecurity Act) pour démontrer la conformité aux exigences. Ces dispositions visent à renforcer la confiance dans la chaîne d'approvisionnement numérique.

Obligations de notification des incidents

NIS 2 durcit et harmonise les exigences de **signalement des incidents** de sécurité. Toute entité essentielle ou importante doit notifier **sans retard injustifié** au CSIRT compétent (ou à l'autorité nationale compétente) **tout incident ayant un impact significatif** sur la fourniture de ses services.

La notion d'« incident significatif » (*important incident*) est définie par la directive : il s'agit d'un incident de nature à causer une perturbation opérationnelle grave de l'activité ou des pertes financières notables pour l'entité, **ou** à affecter d'autres personnes en causant des dommages considérables (matériels ou immatériels).

En pratique, la procédure de notification comporte plusieurs paliers : **une alerte précoce sous 24 heures** après constat de l'incident (pour signaler les faits initiaux et indiquer, par exemple, si une origine malveillante est suspectée) ; puis **une notification détaillée sous 72 heures** au plus tard, apportant une évaluation initiale de l'incident (gravité, impacts, indicateurs de compromission connus). Ensuite, sur demande, des **rapports intermédiaires** doivent être fournis pour tenir informées les autorités de l'évolution de la gestion de l'incident. Enfin, un **rapport final** doit être soumis dans le mois qui suit la notification, avec une analyse complète de l'incident (cause racine, mesures d'atténuation prises, impacts notamment transfrontières). Si l'incident n'est pas totalement résolu dans ce délai, un rapport de progression est exigé et le rapport final est décalé d'un mois supplémentaire après la résolution.

Il convient de noter que notifier un incident aux autorités ne constitue pas en soi une reconnaissance de responsabilité de la part de l'entité, afin d'encourager la transparence. En plus de la notification aux autorités, les entités doivent **informer leurs usagers ou clients** lorsqu'un incident majeur est susceptible de nuire à la fourniture du service afin que ceux-ci puissent réagir en conséquence.

De même, NIS 2 introduit l'obligation d'**alerte sur les menaces** : si une entité découvre une cybermenace significative qui pourrait affecter ses bénéficiaires, elle doit leur communiquer les informations utiles (par exemple des mesures correctives à appliquer) sans retard injustifié.

Ces obligations de notification renforcées visent à améliorer la réactivité du système dans son ensemble et à favoriser le partage d'informations sur les incidents, y compris via le réseau des CSIRT au niveau de l'UE (les points de contact nationaux devant échanger entre eux en cas d'incident transfrontière.

Responsabilités des organes de direction

La directive NIS 2 accorde une attention particulière à la gouvernance de la cybersécurité au sein des organisations. Les **dirigeants et conseils d'administration** des entités couvertes sont explicitement mis à contribution. L'article 20 impose que les *organes de direction* des entités essentielles et importantes **approuvent** les mesures de gestion des risques prises pour se conformer à NIS 2 et **supervisent** leur mise en œuvre.

Ils peuvent être tenus pour **responsables** des manquements à ces obligations de cybersécurité au sein de leur organisation. En clair, la conformité à NIS 2 devient une question de **gouvernance d'entreprise**, impliquant le niveau dirigeant – ce qui est destiné à porter les enjeux de cybersécurité au niveau du conseil d'administration.

Par ailleurs, les membres des organes de direction doivent suivre des **formations en cybersécurité** pour acquérir les compétences nécessaires en matière d'évaluation des risques et de gestion de la sécurité. Les États membres sont tenus de s'assurer que ces formations aient lieu et d'encourager les entités à les étendre à leurs employés clés.

Cette responsabilisation du top management est une innovation notable de NIS 2, visant à ancrer la cybersécurité dans la culture d'entreprise et à garantir un pilotage adéquat des mesures de sécurité au plus haut niveau.

Autres obligations

Outre ce qui précède, NIS 2 comporte d'autres dispositions importantes à caractère réglementaire. Par exemple, la directive encourage la mise en place de programmes de **divulgation coordonnée des vulnérabilités** (pour permettre aux chercheurs en sécurité de signaler des failles de manière responsable) – chaque État membre doit désigner un point de contact pour la divulgation des vulnérabilités et peut obliger les entités à agir suite à la découverte de failles.

De plus, NIS 2 prévoit un cadre de **coopération opérationnelle renforcée** : les CSIRT nationaux doivent disposer de capacités minimales et coopérer activement via le réseau CSIRT, et un mécanisme de gestion de crise cyber (EU-CyCLONe) est institué comme mentionné plus haut.

Enfin, la directive s'articule avec d'autres textes sectoriels : par exemple, le règlement (UE) 2022/2554 (DORA) pour le secteur financier est considéré comme *lex specialis* pour les exigences cyber des entités financières. Ainsi, si une entité est déjà soumise à des exigences au moins équivalentes en vertu d'une législation sectorielle de l'UE, ces exigences prévalent et évitent une double réglementation. Cette clause de non-cumul garantit la cohérence du cadre juridique global de la cybersécurité.

Sanctions et mise en conformité

Pouvoirs de surveillance et d'exécution

Les autorités compétentes doivent disposer des pouvoirs nécessaires pour assurer le respect de la directive, y compris la réalisation d'inspections sur place et la demande d'informations. Elles peuvent émettre des avertissements et imposer des mesures correctives.

Sanctions

La directive NIS 2 prévoit des **sanctions importantes en cas de non-respect de ses dispositions**. Ces sanctions visent à garantir l'efficacité de la directive et à inciter les entités concernées à renforcer leur cybersécurité. Voici les principaux éléments concernant les sanctions :

Sanctions financières (amendes administratives pécuniaires) : La directive NIS 2 introduit un pouvoir de sanction financière, contrairement à NIS 1. Des amendes peuvent être imposées aux entités essentielles (EE) et aux entités importantes (EI) en cas de non-conformité.

- Pour les **entités essentielles (EE)**, les sanctions administratives pécuniaires peuvent atteindre un **maximum d'au moins 10 000 000 EUR ou au moins 2 % du chiffre d'affaires annuel mondial total** de l'entreprise au cours de l'exercice précédent, le montant le plus élevé étant retenu.
- Pour les **entités importantes (EI)**, ces sanctions peuvent atteindre un **maximum d'au moins 7 000 000 EUR ou au moins 1,4 % du chiffre d'affaires annuel mondial total** de l'entreprise au cours de l'exercice précédent, le montant le plus élevé étant retenu.

Ces montants sont des **sanctions minimales** fixées par la Commission européenne, ce qui signifie que chaque État membre peut choisir d'appliquer des pénalités plus élevées.

Des **astreintes** peuvent également être imposées afin de contraindre une EE ou une EI à cesser son infraction.

Autres mesures d'exécution : En plus des sanctions financières, les autorités compétentes disposent d'un éventail de mesures d'exécution pour assurer le respect de la directive. Ces mesures peuvent inclure :

- L'**émission d'avertissements** relatifs aux violations.
- L'**adoption d'instructions contraignantes** pour remédier aux carences ou aux violations, avec des délais d'exécution.
- L'**injonction** aux entités de mettre fin à un comportement non conforme et de s'abstenir de le répéter.
- L'**obligation** pour les entités de mettre en œuvre les recommandations issues d'audits de sécurité.
- La **désignation d'un responsable de contrôle** pour surveiller la conformité.
- L'**obligation de rendre publics certains aspects des violations**.
- La **suspension temporaire** ou la demande de suspension temporaire d'une **certification ou d'une autorisation** relative aux services de l'entité essentielle.
- La demande d'**interdiction temporaire** pour une personne physique exerçant des fonctions de direction au sein de l'entité essentielle d'exercer ces fonctions. Ces suspensions et interdictions ne sont appliquées qu'en dernier recours et jusqu'à ce que l'entité prenne les mesures nécessaires pour remédier aux manquements.

Sanctions pénales : Les États membres peuvent établir des règles relatives aux sanctions pénales en cas de violation des mesures nationales transposant la directive.

Les sanctions prévues par la directive NIS 2 sont donc conçues pour être **dissuasives et proportionnées** à la gravité des infractions et à la taille des entités, afin d'assurer une application effective des mesures de cybersécurité au sein de l'Union européenne.

Responsabilité

La directive NIS 2 implique davantage la direction des entreprises, qui peut être tenue responsable des violations de l'article 21 relatif aux mesures de gestion des risques de cybersécurité. Une obligation de formation et d'implication dans l'application des règles de cybersécurité est également soulignée pour la direction.

Mise en conformité

Pour se conformer à NIS 2, les entités concernées doivent adopter une démarche proactive de renforcement de leur cybersécurité. Dans la pratique, cela implique de **mettre en place un ensemble de mesures organisationnelles et techniques** avant l'échéance d'application de la directive. Parmi les actions concrètes de mise en conformité figurent :

- l'élaboration ou la mise à jour d'une **politique de sécurité informatique interne**,

- la réalisation régulière d'**analyses de risques** IT et l'implémentation des mesures de protection correspondantes (pare-feu, systèmes de détection d'intrusion, sauvegardes, chiffrement, etc.),
- l'établissement de **procédures de gestion d'incident** (plan de réponse, cellules de crise, contacts CSIRT prêts à l'emploi),
- la mise en œuvre d'un **programme de formation et de sensibilisation** du personnel à la cybersécurité,
- ainsi que la **gestion des risques fournisseurs** (cartographie des fournisseurs critiques, intégration de clauses de sécurité dans les contrats, etc.) conformément aux exigences de l'article 21.

Les entreprises doivent également désigner en interne des **responsables de la conformité NIS 2** (par exemple le RSSI – responsable sécurité des systèmes d'information – ou un correspondant dédié) chargés de piloter ces mesures et d'assurer le lien avec les autorités compétentes.

Pour plus d'informations, consultez notre « Plan d'action NIS2 ».

Impact et enjeux

Enjeux globaux

La directive vise à harmoniser les exigences en matière de cybersécurité dans l'ensemble de l'UE. Elle contribue à réduire la fragmentation et à améliorer la coopération transfrontalière. Malgré les efforts nécessaires pour sa mise en conformité, NIS 2 vise à **élever le niveau de cybersécurité en Europe**, en assurant une meilleure résilience face aux cybermenaces, tant pour les entreprises que pour les États.

Pour les entreprises

L'entrée en vigueur de **NIS 2** marque une transformation majeure du cadre réglementaire de la cybersécurité en Europe. Son champ d'application s'élargit considérablement, incluant désormais la majorité des **moyennes et grandes entreprises** de secteurs critiques. Cela signifie que **de nombreuses sociétés auparavant non concernées par NIS 1 doivent désormais se conformer** à des obligations renforcées, impliquant des coûts significatifs :

- Investissements en **mesures de sécurité**
- Renforcement des **équipes IT/cyber**
- Formations et audits

On estime que **des dizaines de milliers d'entreprises** seront concernées à l'échelle européenne, avec par exemple **50 000 entreprises en Italie et 30 000 en Allemagne**.

Les entreprises opérant dans plusieurs pays bénéficieront d'une **harmonisation des règles**, bien que des différences nationales subsistent. La responsabilisation des **dirigeants** devrait également aider à inscrire la cybersécurité parmi les priorités stratégiques.

Pour les états membres

Les **pouvoirs publics** doivent adapter leur cadre législatif pour transposer NIS 2, ce qui implique :

- La désignation d'**autorités compétentes** pour superviser les obligations
- La **mise en place de contrôles et d'un suivi accru** des entreprises concernées
- Une **coordination nationale et européenne** pour éviter des disparités excessives dans l'application de la directive

NIS 2 exige aussi des **capacités opérationnelles renforcées** avec des CSIRT nationaux performants et une coopération accrue via le réseau européen **EU-CyCLONe**.

Enfin, la directive **s'articule avec d'autres réglementations européennes**, notamment la directive **REC 2022/2557** sur la résilience des entités critiques, pour une approche intégrée de la sécurité physique et numérique.

Date d'entrée en vigueur et état d'application

Chronologie de l'entrée en vigueur et de l'application au niveau européen :

27 décembre 2022 : Publication de la directive (UE) 2022/2555 (NIS 2) au Journal officiel de l'Union européenne. La directive est entrée en vigueur le vingtième jour suivant sa publication, soit autour du 16-17 janvier 2023.

17 octobre 2024 : Date limite pour la transposition nationale de la directive par les États membres. À cette date, les États membres devaient avoir adopté et publié les mesures nécessaires pour se conformer à la directive. Ils devaient également communiquer immédiatement à la Commission le texte de ces dispositions.

18 octobre 2024 : Application des mesures nationales. Les États membres doivent appliquer les dispositions nationales transposant la directive à compter de cette date. La directive (UE) 2016/1148 (NIS 1) a été abrogée avec effet à cette date.

17 janvier 2025 : Les États membres doivent communiquer à la Commission européenne les règles relatives aux sanctions applicables en cas de violation des mesures nationales adoptées en application de la directive.

17 avril 2025 : Chaque État membre doit établir une liste des entités essentielles (EE) et des entités importantes (EI) ainsi que des entités fournissant des services d'enregistrement de noms de domaine. Par la suite, les États membres doivent réexaminer périodiquement cette liste, au moins tous les deux ans, et la mettre à jour si nécessaire. Les États membres doivent également notifier à la Commission et au groupe de coopération le nombre d'EE et d'EI pour chaque secteur.

Focus sur la situation en France à date :

15 octobre 2024 : Présentation du projet de loi de transposition de NIS2 en **Conseil des ministres**. Cette présentation intervient deux jours avant la date limite de transposition fixée par l'Union européenne.

15 octobre 2024 : **Dépôt du projet de loi au Sénat** (Texte n° 33), accompagné de l'exposé des motifs, de l'étude d'impact et de l'avis du Conseil d'État.

17 octobre 2024 : **Entrée en vigueur officielle de la directive NIS2 dans le droit français**, mais certaines exigences ne sont pas appliquées immédiatement.

4 mars 2025 : **Travaux en commission spéciale au Sénat**

Dépôt des amendements.

Rapport n° 393 de **Michel Canévet, Patrick Chaize et Hugues Saury**.

Texte de la commission n° 394.

11 et 12 mars 2025 : **Débats en séance publique au Sénat**

Adoption d'amendements et discussions sur le texte.

12 mars 2025 : **Adoption du projet de loi par le Sénat** (Texte n° 78).

13 mars 2025 : **Transmission du texte à l'Assemblée nationale** (Texte n° 1112).

Le gouvernement français a engagé une **procédure accélérée** pour l'examen parlementaire du projet de loi afin de limiter le processus à une seule lecture par chambre, soulignant l'urgence de la mise en œuvre.

L'**ANSSI (Agence Nationale pour la Sécurité des Systèmes d'Informations)** joue un rôle majeur dans la transposition et l'application de la directive en France. L'agence a détaillé une **feuille de route de déploiement progressive**. Elle prévoit d'accorder aux entités régulées un **délai de transition jusqu'à fin 2027 avant d'appliquer des sanctions pour non-conformité complète**.

Cependant, l'Agence fait une distinction entre les obligations. Les mesures considérées comme **rapidement applicables**, notamment **la déclaration des incidents majeurs de cybersécurité**, devront être mises en place **dès l'entrée en vigueur de la loi**. Cette obligation de notification doit se faire dans les **24 heures suivant la détection d'un incident** auprès du CSIRT ou de l'autorité compétente.

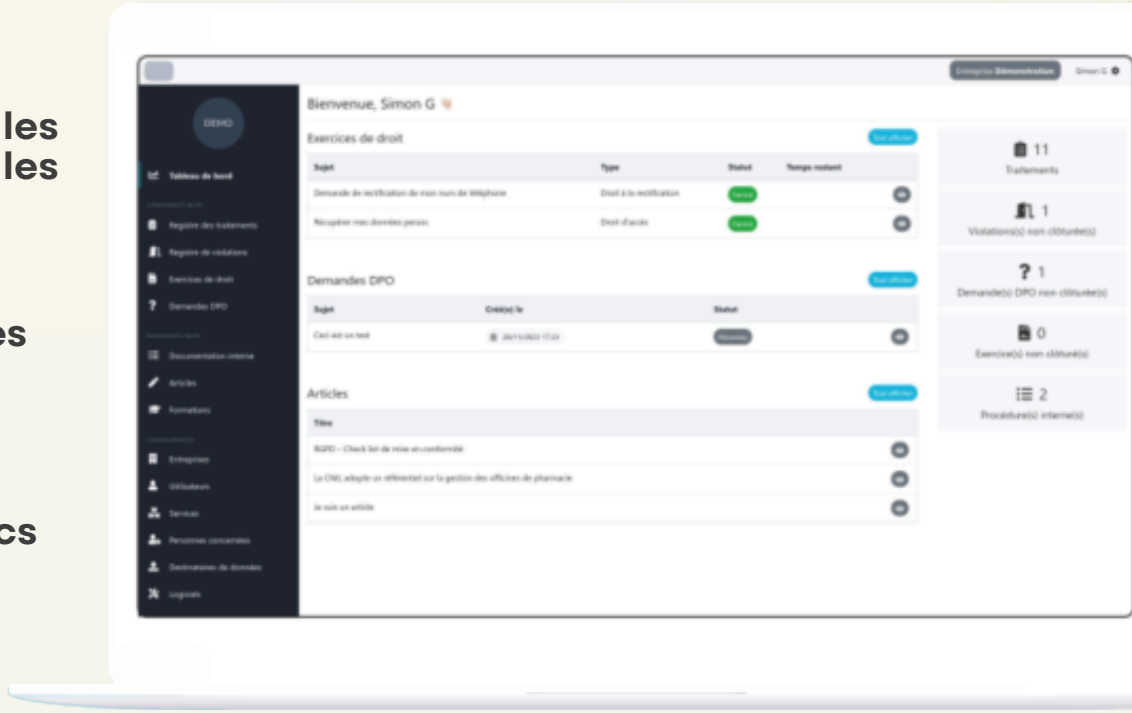
L'ANSSI a reconnu les défis pratiques rencontrés par de nombreuses structures, notamment en termes de contraintes budgétaires et de manque de compétences techniques, et insiste sur la nécessité d'un **accompagnement renforcé de l'État**.

PRODPO - LE LOGICIEL IDÉAL DU DPO

Simplifier la gestion de conformité RGPD dans votre organisation

ProDPO est une solution logicielle conçue pour les Délégués à la Protection des Données (DPO) et les professionnels du RGPD.

- **Interface intuitive et fonctionnalités avancées**
- **Registre de traitement personnalisable**
- **Gestion intégrée des exercices des droits**
- **Gestion des violations et AIPD en quelques clics**

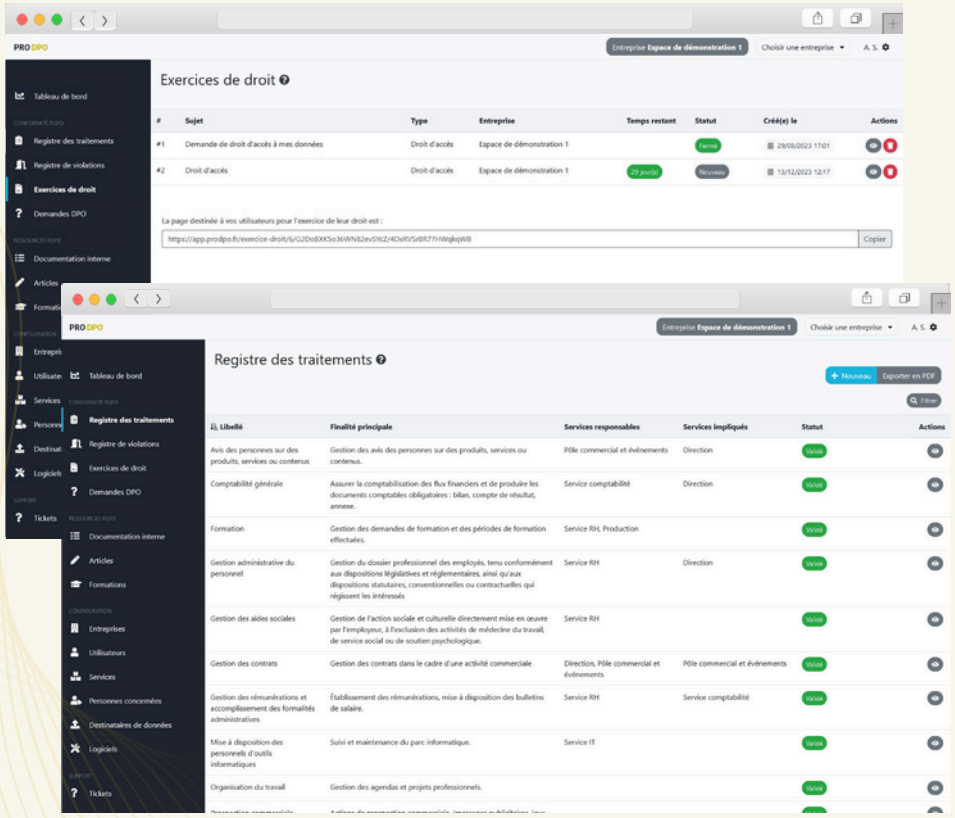


Vous êtes DPO au sein de votre entreprise ou DPO externe de plusieurs organisations, ce logiciel a été pensé pour vous.

PRODPO

FONCTIONNALITÉS INNOVANTES

POUR UNE GESTION RGPD EFFICACE



Registre de traitement

ProDPO personnalise et préconfigure un registre des activités de traitement pour vous. Le logiciel intègre une base de traitements standards adaptée à votre secteur ou à ceux de vos clients.

Tableau de bord intuitif

ProDPO vous propose une vue d'ensemble conçue pour offrir une compréhension instantanée, ce tableau de bord transforme les données complexes en insights actionnables.

Gestion des exercices des droits

ProDPO révolutionne la gestion des exercices de droits avec un formulaire personnalisé pour votre entreprise ou celle de vos clients. Cette centralisation permet une gestion efficace et transparente des demandes des personnes concernées.

ProDPO n'est pas seulement un logiciel, c'est un partenaire stratégique dans la protection et la gestion des données personnelles.

FONCTIONNALITÉS INNOVANTES

POUR UNE GESTION RGPD EFFICACE

Gestion des violations de données

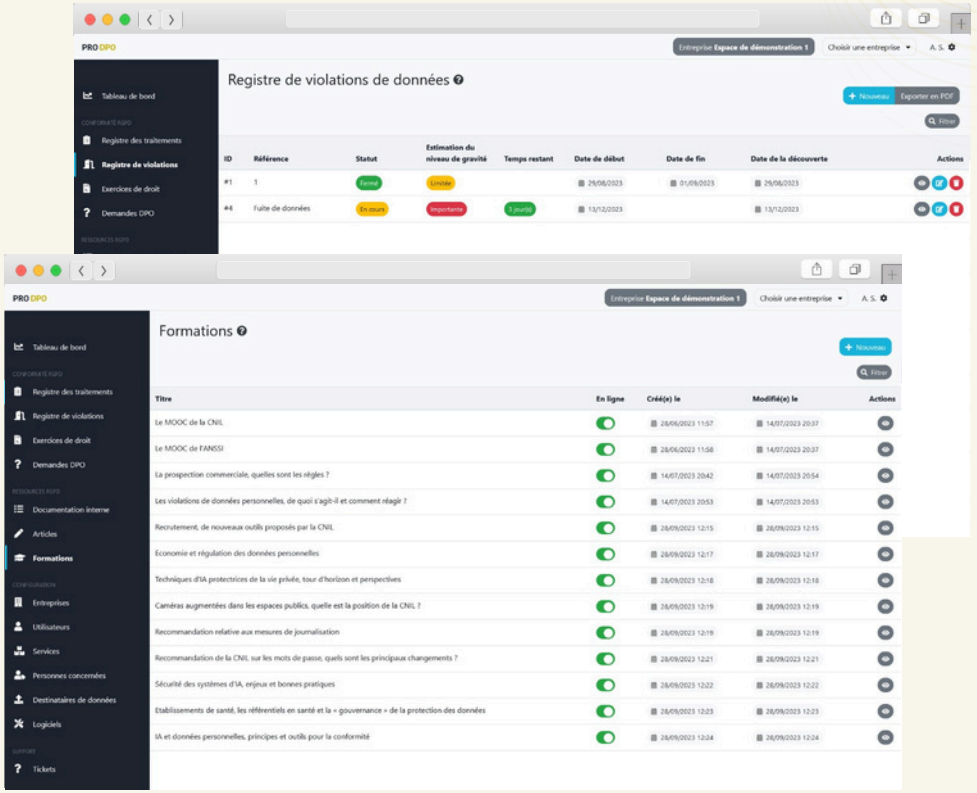
Face à une violation de données, la réactivité est cruciale. ProDPO vous permet de gérer efficacement ces situations critiques en vous aidant à documenter la violation et à préparer vos déclarations à la CNIL.

Documentation RGPD

ProDPO sera votre bibliothèque centralisée de procédures et de documentations RGPD. Organisez et stockez tous vos documents, et facilitez la signature électronique par vos collaborateurs.

Formation RGPD et Cybersécurité

Grâce à des contenus gratuits et régulièrement mis à jour, ProDPO va au-delà de la simple conformité en intégrant une plateforme de formation sur le RGPD et la cybersécurité.



ProDPO n'est pas seulement un logiciel, c'est un partenaire stratégique dans la protection et la gestion des données personnelles.

NOS OFFRES

Abonnements flexibles

FORMULE DPO INTERNE

Parfaite pour les DPO opérant en interne, cette formule offre un accès illimité aux utilisateurs et inclut toutes les fonctionnalités essentielles pour une gestion complète de la conformité RGPD.

À partir de 28 € / mois

FORMULE DPO EXTERNE OU MUTUALISÉ

Cette formule transforme la gestion de la conformité RGPD grâce à une plateforme unique permettant de gérer tous vos comptes clients.

Elle optimise le passage d'un client à l'autre pour un gain de temps et d'efficacité. Elle permet aussi d'enrichir la base standard avec des traitements spécifiques à chacun des secteurs de vos clients, offrant une gestion de la conformité sur mesure.

ProDPO s'adapte et évolue selon vos besoins, quelle que soit la taille de votre entreprise.

À partir de 28 € / mois - Prix dégressif

ProDPO est plus qu'un logiciel de conformité RGPD ; c'est un écosystème complet qui équipe les DPO et les entreprises avec les outils nécessaires pour naviguer avec confiance dans le paysage complexe de la protection des données.

En choisissant ProDPO, vous optez pour une solution qui allie innovation, sécurité, et expertise pour transformer la manière dont votre organisation gère la conformité RGPD.

Rejoignez les organisations qui font confiance à ProDPO pour leur conformité RGPD. Contactez-nous dès aujourd'hui pour une démonstration personnalisée et découvrez comment ProDPO peut transformer la gestion de vos données.

WWW.PRODPO.FR