Consultation sur le projet de recommandation sur le déploiement d'un serveur mandataire web filtrant

Synthèse des contributions

Mars 2025

Du 28 juillet au 30 septembre 2025, la CNIL a lancé une consultation publique sur son projet de recommandation sur le déploiement d'un serveur mandataire web filtrant afin de recueillir les difficultés d'interprétation suscitées par le texte. Les contributions ont nourri les travaux de la CNIL en vue de la publication de la recommandation.

CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

Synthèse des contributions

Cette consultation publique a majoritairement fait l'objet de contributions de la part de professionnels de la sécurité des données et des systèmes d'information pouvant occuper différentes responsabilités, notamment DPO/DPD, RSSI, consultants et ingénieurs en cybersécurité ou responsables d'organismes.

À propos de la consultation publique de la CNIL sur le projet de recommandation

La numérisation croissante de l'activité économique – y compris dans le secteur public – s'accompagne d'une nette augmentation des menaces cyber, qui se professionnalisent. Les solutions pour y faire face ont évolué pour une sécurité en profondeur basée sur des technologies mêlant intelligence artificielle, mutualisation et utilisation d'informations diverses, prise de décision automatisée, ou encore analyse du comportement des utilisateurs pour les plus avancées.

Ces solutions, comme les serveurs mandataires web filtrant, peuvent permettre de répondre notamment à l'obligation de sécurité des données (article 32 du règlement général sur la protection des données ou RGPD). Cependant, elles reposent elles-mêmes sur des traitements de données dont la conformité au RGPD doit aussi être assurée.

Afin d'accompagner les acteurs, la CNIL prévoit l'adoption d'une recommandation sur le déploiement d'un serveur mandataire web filtrant. Le but est de sécuriser les responsables de traitement – utilisateurs de telles solutions – et d'encourager les fournisseurs à adopter une approche de protection des données dès la conception.

Un projet de recommandation a été publié sur le site de la CNIL du 28 juillet 2025 au 30 septembre 2025 afin de recueillir les retours de l'écosystème. Ceux-ci ont été analysés et pris en compte lors de l'édition de la version finale de la recommandation.

Quelques chiffres sur les participants

14 contributions provenant de contributeurs issus de divers secteurs d'activité ont été reçues suite à la consultation :

- 1 administration publique ;
- 4 éditeurs ;
- 4 entreprises privées ou fédérations de professionnels ;
- 1 association ;
- 4 établissements publics.

Parmi les participants, 4 étaient DPO, 6 avaient un poste lié à la sécurité des systèmes d'information et 2 avaient un poste de direction.

Principales évolutions suite aux retours de la consultation

Sur le périmètre et sur les termes

- Dans un souci de cohérence avec le terme couramment employé, notamment par l'ANSSI, la recommandation emploie maintenant celui de **serveur mandataire web filtrant** (et non pas la passerelle de filtrage web).
- S'agissant du périmètre de la recommandation, il a été précisé que celle-ci était strictement **limitée au serveur mandataire web filtrant déployé dans un cadre professionnel**. Les solutions de WAF, de DLP et d'EDR sont hors périmètre. De même, le sujet du filtrage web sur les réseaux Wi-Fi publics a déjà fait l'objet d'une communication de la CNIL et n'est pas l'objet de cette recommandation.

Sur la structure et le fond

- La section *2. Qu'est-ce qu'un serveur mandataire web filtrant ?* a été simplifiée par un **redécoupage des catégories d'objectifs et fonctionnalités pour ne retenir que des fonctions**.
- La formulation liée à l'analyse antivirus/antimalware a évolué pour être plus neutre sur la technologie employée pour la détection et le blocage de pages web et fichiers malveillants.
- Au titre des finalités du traitement, il a été rappelé que la **mise en œuvre de ces traitements ne doit pas conduire à une surveillance excessive** de l'activité des salariés qui serait contraire, notamment, au RGPD.
- Le **rôle central du DPO** a été réaffirmé comme partie prenante dans le déploiement d'une telle solution.
- La fonction de filtrage web a été ouverte à la **restriction non bloquante**.
- Il a été **précisé les informations que le responsable de traitement doit fournir aux personnes concernées, notamment concernant l'absence de conservation des contenus échangés** hors charge malveillante. Cette conservation peut permettre la réalisation d'une analyse en cas d'incident de sécurité.