silex | PROTECTION DES DONNÉES ET CYBERSÉCURITÉ

CHECKLIST

Préparation et gestion d'un contrôle CNIL

1 | Mieux connaître la CNIL et les procédures de contrôle

Comprendre les motifs de contrôle

Action	Détails
Identifier les sources de déclenchement	Les contrôles sont réalisés à l'initiative de la Présidente de la CNIL. Les origines fréquentes sont : • Les signalements/réclamations reçus, • Les plaintes dues à l'absence de réponse à l'exercice des droits, • L'initiative directe de la CNIL (basée sur les thématiques prioritaires annuelles, ex : prospection commerciale, cloud, IA, cybersécurité, applications mobiles), • Ou les suites de précédentes procédures/sanctions.
Connaître les types de contrôle	La CNIL utilise quatre méthodes, qui peuvent être complémentaires : • **Sur place** : Les contrôleurs se rendent dans les locaux, généralement de manière inopinée. • **Sur convocation** : Le personnel est convoqué dans les locaux de la CNIL pour être interrogé. • **Sur pièces** : L'établissement répond à un questionnaire par courrier en fournissant des justificatifs. • **À distance/en ligne** : La CNIL effectue des vérifications sur des données librement accessibles en ligne (ex : audit de site internet).
Savoir ce que la CNIL cherche à vérifier	Lors des vérifications, une attention particulière est portée sur : • La finalité des traitements et leur base légale. • La nature des données collectées, notamment au regard du principe de minimisation. • Les modalités d'information des personnes concernées. • Les durées de conservation des données personnelles. • Les moyens mis en œuvre pour préserver la sécurité des données personnelles. • Les destinataires des données et les éventuels transferts hors de l'Union européenne.
Identifier les risques de sanction	Les manquements les plus constatés incluent le défaut de coopération avec la CNIL et le non-respect de l'exercice des droits des personnes concernées. Les amendes peuvent s'élever jusqu'à 4 % du chiffre d'affaires annuel mondial.

2 | Anticiper et préparer un contrôle

Gouvernance et organisation

Action	Détails	Check
Identifier les sources de déclenchement	Les contrôles sont réalisés à l'initiative de la Présidente de la CNIL. Les origines fréquentes sont : • Les signalements/réclamations reçus, • Les plaintes dues à l'absence de réponse à l'exercice des droits, • L'initiative directe de la CNIL (basée sur les thématiques prioritaires annuelles, ex : prospection commerciale, cloud, IA, cybersécurité, applications mobiles), • Ou les suites de précédentes procédures/sanctions.	☐
Adopter une démarche de conformité dynamique	La manière la plus efficace d'être prêt est de s'être inscrit dans une démarche de mise en conformité dynamique et permanente pour assurer une protection des données continue.	☐
Réaliser un audit interne régulier	Évaluer votre niveau de maturité et identifier les points forts et les faiblesses de votre système de gestion des données personnelles. Utiliser si possible l'auto-évaluation de maturité de la CNIL.	☐
Nommer et impliquer le DPO	Le Délégué à la Protection des Données (DPO) joue un rôle central dans la mise en conformité et est l'interlocuteur privilégié pour faciliter l'accès de la CNIL aux documents.	☐
Former et sensibiliser le personnel	Sensibiliser l'ensemble du personnel aux enjeux du RGPD et aux bonnes pratiques. Former spécifiquement les agents d'accueil et de sécurité à la procédure à suivre en cas de contrôle inopiné.	☐
Définir une procédure interne de crise	Préparer une procédure décrivant comment réagir en cas de contrôle. Cette procédure doit décrire : • Les modalités de déroulement (recueil de pièces, entretiens, PV). • Les prérogatives des agents de la CNIL. • Les obligations et le périmètre de chaque acteur. • Les actions à réaliser pendant et après le contrôle.	☐
Désigner les référents internes (cellule de crise)	Identifier *en amont* les personnes clés à prévenir et à mobiliser immédiatement (DPO, DSI, RSSI, chefs de service, responsable des lieux, conseil juridique). Prévoir au moins deux personnes par service pour pallier les absences.	☐

Assurer une base documentaire solide

Action	Détails	Check
Centraliser la documentation de conformité	Organiser et centraliser la gestion et l'accès à toute la documentation pour qu'elle soit rapidement disponible aux intervenants (DPO, RSSI, DSI, etc.).	☐
Tenir à jour les registres obligatoires	Disposer du Registre des activités de traitement (RT) et de sous-traitance (ST).	☐
Disposer des analyses de risque et d'impact	Avoir réalisé et documenté les Analyses d'Impact sur la Protection des Données (AIPD) pour les traitements présentant des risques élevés.	☐
Documenter la gestion des droits et incidents	Maintenir le Registre des Demandes d'exercice de droits et le Registre des Violations de données personnelles.	☐
Disposer des preuves légales	Avoir à disposition les modèles de recueil de consentement et les preuves que les personnes concernées ont donné leur consentement lorsque c'est la base légale.	☐
Avoir les documents contractuels et sécuritaires	Avoir des contrats de sous-traitance à jour, ainsi que la Politique de Sécurité des Systèmes d'Information (PSSI) et les mesures de sécurité mises en place.	☐

3 | Encadrer le jour du contrôle

Vérifications initiales et mobilisation des équipes

Action	Détails	Check
Vérifier les documents d'habilitation	S'assurer de la présence et de l'identité des contrôleurs en sollicitant leurs cartes professionnelles, l'ordre de mission, et la décision de la Présidente de la CNIL précisant l'objet des vérifications.	☐
Identifier le responsable des lieux	Désigner rapidement le responsable des lieux (souvent le responsable de traitement), qui sera l'interlocuteur privilégié pour accompagner la délégation.	☐
Activer la procédure de crise	Informer immédiatement la direction et la cellule de crise (DPO, RSSI, DSI).	☐
Aménager la logistique	Mettre rapidement à disposition des agents une salle de réunion dédiée pour qu'ils puissent s'isoler pour rédiger le procès-verbal, ainsi que les moyens matériels (imprimante, accès sécurisé aux fichiers).	☐
Préparer les interlocuteurs	S'assurer de la disponibilité des personnes pertinentes pour les entretiens, et préparer si possible une brève synthèse sur le traitement objet du contrôle.	☐

Attitude et coopération

Action	Détails	Check
Coopérer et répondre loyalement	L'organisme est tenu de coopérer, en fournissant des réponses complètes, loyales, factuelles, claires, synthétiques et précises.	☐
Éviter l'entrave	Ne pas entraver l'action de la CNIL (ex : ne pas modifier ou dissimuler des documents ou éléments). L'entrave est passible de sanctions pénales.	☐
Ne pas divulguer d'informations protégées	Ne pas remettre de documents couverts par le secret professionnel avocat/client ou le secret médical, sauf si la délégation est accompagnée d'un médecin.	☐
Rester dans le périmètre du contrôle	Ne fournir que les documents demandés et s'assurer que les demandes de la CNIL restent dans le périmètre défini par la décision de contrôle, si nécessaire, en discutant les limites.	☐
Assistance juridique	Exercer le droit de se faire assister par un conseil (avocat, DPO externe) pendant le contrôle, y compris lors des auditions.	☐
Documenter les échanges	Noter au fur et à mesure l'ensemble des documents demandés par la délégation et ceux effectivement transmis sur place ou à communiquer ultérieurement.	☐

Clôture des opérations de contrôle

Action	Détails	Check
Examiner le Procès-Verbal (PV)	À l'issue des opérations (sauf contrôle sur pièces), un procès-verbal est systématiquement dressé. Le responsable des lieux doit le relire très attentivement avant de le signer.	☐
Formuler des observations	Le responsable peut formuler d'éventuels commentaires ou observations sur le PV, notamment si la retranscription des échanges n'est pas fidèle. ***C'est votre unique opportunité de façonner le récit officiel de l'inspection. Toute omission ou interprétation erronée qui n'est pas corrigée dans ce document devient la "vérité administrative" !***	☐
Obtenir une copie	S'assurer d'obtenir une copie de la version finale du procès-verbal incluant toutes les pièces et informations recueillies.	☐

4 | Gérer l'après-contrôle et éviter les sanctions

Suivi immédiat post-contrôle

Action	Détails	Check
Transmettre les pièces complémentaires	Communiquer à la délégation les documents complémentaires mentionnés dans le PV dans les délais impartis, en utilisant une solution de partage de fichiers sécurisée.	☐
Analyser les constatations	Le responsable des traitements doit analyser attentivement les conclusions du contrôle et prendre en compte les constatations et observations figurant au procès-verbal dans les meilleurs délais.	☐
Faire un bilan interne	Organiser des réunions en interne pour un premier bilan, et envoyer à la direction un rapport avec des propositions d'actions correctives.	☐

Mesures correctives et conformité

Action	Détails	Check
Élaborer un plan d'action	Si des points de non-conformité sont identifiés, élaborer un plan d'action visant à intégrer les enseignements tirés du contrôle et corriger les lacunes.	☐
Mise en œuvre rapide des corrections	Mettre en œuvre les mesures correctrices dans les plus brefs délais et suivre le respect des échéances.	☐
Coopération post-contrôle	Continuer de fournir à la CNIL des informations sur les mesures réalisées suite au contrôle pendant toute la durée de l'instruction du dossier.	☐
Anticiper les suites	L'organisme doit anticiper les suites possibles (clôture avec recommandations, avertissement, mise en demeure).	☐

Répondre à une mise en demeure, le cas échéant

Action	Détails	Check
Respecter le délai imparti	Si l'organisme reçoit une mise en demeure, il doit se conformer à la réglementation dans le délai imparti et *démontrer l'effectivité* des mesures mises en œuvre.	☐
Éviter la sanction	L'absence de réponse à une mise en demeure ou l'absence de mise en conformité dans le délai fixé peut entraîner la transmission du dossier à la formation restreinte de la CNIL, qui peut prononcer des sanctions pécuniaires (amendes) ou non pécuniaires (rappel à l'ordre, injonction).	☐
Amélioration continue	L'étape de suivi post-contrôle est une opportunité pour renforcer les processus internes et consolider la culture de protection des données, favorisant une amélioration continue.	☐

silex | PROTECTION DES DONNÉES ET CYBERSÉCURITÉ

EXPERTISE

PROTECTION DES DONNÉES

silex | PROTECTION DES DONNÉES ET CYBERSÉCURITÉ

CABINET DE CONSEIL
DPO EXTERNE

Notre cabinet est spécialisé dans le conseil RGPD auprès des entreprises, institutions publiques et associations :

- Informer, conseiller et guider pour respecter le règlement européen et le droit national sur la protection des données
- Sensibiliser vos équipes aux enjeux de la protection des données personnelles
- Superviser les audits internes sur la protection des données
- Conseiller et assurer la mise en œuvre de l'analyse d'impact sur la vie privée
- Répondre aux questions et réclamations liées à la protection des données
- Vous soutenir en cas de violation des données et dans la gestion de crise
- Coopérer avec la CNIL en tant que point de contact au sein de votre structure

silex | PROTECTION DES DONNÉES ET CYBERSÉCURITÉ

NOTRE ÉQUIPE D'EXPERTS

NINON MAIRE

Consultant RGPD Sénior

Master 2 en Droit du numérique

LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG
Centre de gestion du personnel
et de l'organisation de l'État

ALEXIS GABRY

Consultant RGPD Sénior

Master 2 en Droit du numérique

devoteam

CNIL.

ARTHUR RENARD

Consultant RGPD Sénior

Master 2 en Droit du numérique

CORUM BUTLER

silexo | PROTECTION DES DONNÉES ET CYBERSÉCURITÉ

ATOUTS & RÉFÉRENCES

Pour répondre au mieux à vos besoins, nous mettons à votre disposition l'un de nos DPO seniors.

Ils s'appuiera sur les outils, les méthodologies éprouvées ainsi que sur l'expertise collective de l'ensemble des collaborateurs du cabinet SILEXO.

Notre équipe a déjà accompagné plus de 65 organisations dans leurs démarches de conformité, dans des secteurs variés, et notamment :

SECTEURS DIVERS

ZENITUDE HÔTEL-RÉSIDENCES

VALUE

rtb régie des transports du Territoire de Belfort

LEO & ASSOCIÉS Assurance | Audit | Conseil

INTERNATIONAL - MULTISITE

l'alliance mutualiste

DELFINGEN

ARCHEON MEDICAL

PRÉVOIR Assureur Solutions Vie

CONTACTS

silexo | PROTECTION DES DONNÉES ET CYBERSÉCURITÉ

Conseil I Audit I Formation I DPO Externe

Pour en savoir plus : www.silexo.fr

Échangeons : rdv-alexis-gabry.silexo.fr