Autoévaluation de maturité en gestion de la protection des données

Un modèle pour se positionner et choisir les actions à mener

CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

Table des matières

Le concept de maturité appliqué à la protection des données personnelles

La protection des données repose sur des activités mises en œuvre par chaque organisme (pilotage, gestion du registre, veille juridique, etc.). Toutefois, ces activités n'existent pas dans toutes les entreprises et ne sont pas toujours gérées de manière homogène (informelles, décrites, généralisées, etc.).

Ce document propose un modèle, dit de maturité, qui quantifie la rigueur et le formalisme avec laquelle les activités liées à la gestion de la protection des données sont gérées.

L'objectif de ce document est de :

1. **Transposer la notion de niveaux de maturité, déjà bien définie (ex. : ISO/IEC 21827, guide « maturité SSI »), à la protection des données.**
2. **Proposer des activités types liées à la protection des données.**
3. **Illustrer chaque niveau de maturité pour chaque activité type par des exemples d'actions ou de productions.**

Note : alors que la conformité s'applique à des traitements de données personnelles, la maturité s'applique à des activités. Ces deux visions sont différentes mais complémentaires.

1. Cinq niveaux de maturité pour évaluer la manière dont sont gérés les processus liés à la protection des données

Dans le domaine de la protection des données, les différents niveaux de maturité correspondent à ceux définis dans l'ISO/IEC 21827 et le guide « maturité SSI » de l'ANSSI.

Le tableau suivant décrit les cinq niveaux de maturité de manière générique. Chaque niveau représente la manière dont un organisme conçoit, met en œuvre, contrôle, maintient et assure le suivi d'une activité, quel que soit cette activité. L'atteinte d'un niveau suppose d'avoir déjà atteint le niveau précédent.

Niveaux		Caractéristiques
0	**Pratique inexistante ou incomplète**	Rien n'est fait en matière de protection des données. Celle-ci n'est pas connue ni prise en charge au sein de l'organisme et le besoin n'est pas reconnu.
1	**Pratique informelle** (quelques actions isolées)	☐ Des actions sont réalisées en employant des pratiques de base. Elles sont mises en œuvre de manière informelle et en réaction à des demandes isolées, sans réel engagement des dirigeants de l'organisme ni réelle coordination entre ceux qui mettent en œuvre ces actions.
2	**Pratique répétable et suivie** (des actions reproductibles)	☐ Les actions sont réalisées par une personne qui possède des compétences en protection des données. ☐ Les actions sont planifiées. ☐ Quelques pratiques sont formalisées, ce qui permet la duplication et la réutilisation (éventuellement par une autre personne). ☐ La protection des données est suivie par les dirigeants de l'organisme, mais tout le métier est loin de s'être impliqué. ☐ Des mesures qualitatives sont réalisées (indicateurs simples sur les résultats, ex : considération de la protection des données dans tel ou tel projet).
3	**Processus défini** (standardisation des pratiques)	☐ Les actions sont réalisées conformément à un processus défini (ex. : emploi de méthodes), standardisé (commun à tout l'organisme) et formalisé (existence d'une documentation). ☐ Les personnes réalisant les actions possèdent les compétences appropriées au processus. ☐ L'organisme soutient le processus (il accorde les ressources, les moyens et la formation nécessaires à son fonctionnement). ☐ Le processus est bien compris autant par le management que par les exécutants.
4	**Processus contrôlé** (mesure quantitative et correction des défauts)	☐ Le processus est coordonné dans tout le périmètre choisi et pour chaque exécution. ☐ Des mesures quantitatives sont régulièrement effectuées (en termes de performance, ex. : proportion de projets considérant la protection des données). ☐ Les mesures effectuées (indicateurs qualitatifs et quantitatifs) sont analysées (ex. : quelqu'un est chargé d'étudier les indicateurs et de proposer une analyse et un plan d'action). ☐ Des améliorations sont apportées au processus à partir de l'analyse des mesures effectuées.
5	**Processus continuellement optimisé** (amélioration continue)	☐ Le processus est adapté de façon dynamique à la situation (améliorations et changements directement intégrés). ☐ L'analyse des mesures effectuées est définie, standardisée et formalisée. ☐ L'amélioration du processus est définie, standardisée et formalisée. ☐ Les évolutions du processus sont tracées.

2. Huit activités types liées à la protection des données pour structurer les actions menées

De manière générique, les activités liées à la protection des données sont les suivantes (que l'on peut théoriquement retrouver dans tout organisme, qu'ils soient réellement mis en œuvre ou non) :

Actions	Caractéristiques	Responsables généralement impliqués
Définir et mettre en œuvre des procédures de protection des données	Définition, tenue à jour et communication des politiques et procédures générales relatives à la gestion des données personnelles et à la protection de la vie privée (charte d'utilisation du système d'information, clauses contractuelles types, etc.), vérification de leur application et déclenchement des éventuelles mesures prévues en cas de manquement.	*Définition* par la direction juridique, direction des risques ou direction des systèmes d'information, *vérification* via les processus de contrôle interne.
Piloter la gouvernance de la protection des données	Définition, mise en place, mise en œuvre, communication et amélioration de la stratégie de protection des données au sein de l'organisme (gouvernance, rôles et responsabilités, y compris ceux du délégué à la protection des données – DPO).	Direction générale de l'entreprise et, selon les organismes, pilotage et mise en œuvre par la direction juridique, la direction des risques ou la direction des systèmes d'information.
Recenser et tenir à jour la liste des traitements	Identification et tenue à jour de l'inventaire des traitements de données personnelles, des données et des flux de données qui leurs sont associés.	Délégué à la protection des données (DPO)
Assurer la conformité juridique des traitements	Évaluation des traitements de données personnelles existants ou en projet au regard des obligations légales et réglementaires en matière de protection des données (proportionnalité et nécessité, ainsi que droits des personnes), détermination de mesures pour améliorer la conformité (y compris des clauses contractuelles types), conseil au responsable de traitement et vérification de la mise en œuvre des mesures prévues.	Directions métiers concernées, direction juridique, direction des achats, DPO, responsable de la sécurité des systèmes d'information (RSSI), équipes projet
Former et sensibiliser	Diffusion de la connaissance et création ou renforcement des compétences internes concernant la protection des données. Note : les sessions de formation/sensibilisation doivent permettre de garantir la bonne connaissance de la politique de protection des données de la part du personnel.	DPO, direction des ressources humaines, direction de la communication.
Traiter les demandes des usagers internes et externes	Définition, mise en place, mise en œuvre et communication des moyens permettant la gestion des demandes d'exercice des droits des personnes concernées (ex : demandes de droit d'accès), des plaintes et autres réclamations internes et externes concernant la protection des données.	DPO
Gérer les risques de sécurité	Appréciation des risques de sécurité que les traitements de données personnelles sont susceptibles d'engendrer sur les personnes concernées, détermination de mesures contribuant à les traiter (y compris des clauses contractuelles types) et vérification de la mise en œuvre des mesures prévues.	Directions métiers concernées, direction juridique, direction des achats, DPO, responsable de la sécurité des systèmes d'information (RSSI), équipes projet.
Gérer les violations de données	Identification, qualification, résolution des violations de données personnelles, notifications aux autorités de protection de données et communication aux personnes concernées, tenue d'un registre des violations.	DPO, directions métiers concernées, direction des risques, direction des systèmes d'information, direction de la communication, entités chargées de la gestion des incidents et de la gestion de crise.

3. Les niveaux de maturité appliqués aux activités liées à la protection des données

Le tableau suivant illustre chaque niveau de maturité de chaque activité liée à la protection des données par **des exemples de constats**.

	1 Pratique informelle	2 Pratique répétable et suivie	3 Processus défini	4 Processus contrôlé	5 Processus continuellement optimisé
Définir et mettre en œuvre des procédures sur la protection des données	Quelques bonnes pratiques sont ponctuellement mises en œuvre (ex. : minimisation de la collecte ou effacement des données obsolètes, mentions d'information).	Des documents relatifs à la protection des données (bonnes pratiques, règles, exemples, etc.) sont partagés. Il existe une documentation (ex. : charte d'utilisation des moyens informatiques) comportant des règles relatives à la protection des données.	Une documentation formelle (ex. : politique de protection des données), approuvée par le comité de direction, est communiquée à l'ensemble du personnel. Des procédures sont formalisées et transmises à l'ensemble du personnel. Les règles sont appliquées.	Une revue annuelle des politiques et procédures est réalisée. Des indicateurs sont produits (ex. : sur la mise en œuvre des règles, sur les difficultés rencontrées, sur leur efficacité, etc.).	Les politiques et procédures sont mises à jour dès identification d'une amélioration possible.
Piloter la gouvernance de la protection des données	Des compétences relatives à la protection des données sont identifiées au sein de l'organisme (ex : service juridique) et exploitées ponctuellement.	Un responsable des questions relatives à la protection des données, chargé notamment des interactions avec les personnes concernées (courriers, etc.), est identifié.	Un délégué à la protection des données est désigné auprès de l'autorité nationale de protection des données personnelles (avec une fiche de poste ou une lettre de mission formelle et connue du personnel), une organisation est mise en place et les rôles et responsabilités sont définis.	Le délégué à la protection des données fait un bilan annuel de ses actions aux dirigeants de l'organisme (notamment le(s) responsable(s) de traitements).	Des moyens sont régulièrement alloués pour mettre en œuvre des plans d'action au regard du bilan du délégué à la protection des données et s'assurer de leur mise en œuvre et de leur amélioration continue.
Recenser et tenir à jour la liste des traitements	Les services sont capables d'identifier les traitements de données personnelles qu'ils mettent en œuvre.	Les traitements de données personnelles sont identifiés et/ou signalés de manière centralisée.	Un registre des activités de traitement, conforme au RGPD, est tenu.	La complétude et la qualité du registre sont régulièrement vérifiées.	Le registre sert d'instrument de pilotage des actions relatives aux traitements de données personnelles (ex. : il sert de recensement, mais aussi d'instrument de gestion comparative des risques et de suivi des plans d'action).
Assurer la conformité juridique des traitements	Une information des personnes (ex : mentions légales) est faite sur les principaux endroits de collecte de données personnelles (ex : site web, formulaires).	Pour chaque traitement, des mentions légales sont réalisées et une étude des principes fondamentaux (proportionnalité, nécessité et droits des personnes) est menée. Les clauses contractuelles sont évaluées et comprennent une partie relative à la protection des données.	Des clauses types pour les contrats avec les sous-traitants sont formalisées et utilisées. Des analyses d'impact relatives à la protection des données sont menées sur les traitements susceptibles d'engendrer des risques élevés sur les personnes, en collaboration avec les services concernés et la personne en charge de la protection des données.	Les mesures prévues sont vérifiées. Des revues régulières des mentions légales et des clauses contractuelles sont programmées et réalisées. La qualité des analyses d'impact relatives à la protection des données est évaluée par des indicateurs. Des plans d'action (ex : en cas de non-conformité d'un traitement) sont créés et mis en œuvre.	La protection des données est prise en compte dès l'initiation des projets, en collaboration avec le délégué à la protection des données. Les améliorations possibles sont régulièrement étudiées. Une veille juridique et technique est réalisée. Des analyses sont produites et diffusées.

	1 Pratique informelle	2 Pratique répétable et suivie	3 Processus défini	4 Processus contrôlé	5 Processus continuellement optimisé
Former et sensibiliser	Certains collaborateurs sont sensibilisés à la protection des données.	Les métiers sont formés à identifier et transmettre les sujets liés à la protection des données à la personne en charge (ex. : demandes des personnes concernées, de l'autorité de contrôle, nouveaux traitements, etc.).	Des sessions de sensibilisation sont régulièrement organisées pour le personnel.	Des indicateurs mesurent qualitativement et quantitativement la compréhension des sujets liés à la protection des données (ex. : sondage, questionnaire annuel, etc.).	Des formations ou sessions d'information sont régulièrement proposées sur de nouvelles technologies ou problématiques relatives à la protection des données.
Traiter les demandes des usagers internes et externes	Les demandes des usagers sont gérées au cas par cas.	Des courriers types sont créés (ex. : à partir des modèles de la CNIL) pour répondre aux demandes régulièrement effectuées.	Des réponses types aux demandes d'exercice des droits et questions sont créées et utilisées. Une procédure de gestions des demandes d'exercice de droits est définie et communiquée au personnel. Un formulaire de contact est mis en place sur le site internet et toutes les requêtes sont centralisées.	La personne en charge de la protection des données est systématiquement informée de chacune des demandes concernant le droit des personnes. Les demandes d'exercice des droits font l'objet d'indicateurs qui apparaissent dans le bilan annuel.	Le processus de gestion des demandes d'exercice des droits et les outils sur lesquels il repose font régulièrement l'objet d'améliorations.
Gérer les risques de sécurité	Des mesures de sécurité élémentaires sont mises en place (ex. : habilitations, sécurisation des postes de travail, etc.).	Des référentiels sont utilisés pour choisir et mettre en place des mesures de sécurité (ex. : Guide sécurité des données personnelles de la CNIL, politique de sécurité interne, etc.).	Les analyses d'impact relatives à la protection des données (AIPD) comprennent une étude des risques de sécurité. Une méthode est employée pour apprécier les risques des traitements susceptibles d'engendrer des risques élevés sur les personnes concernées et les traiter de manière proportionnée. Les études de risques font l'objet de plans d'action.	La mise en œuvre des plans d'action est vérifiée en termes d'effectivité et d'efficacité. Les risques résiduels sont suivis par des indicateurs.	Les études de risques et plans d'action font l'objet d'une revue annuelle. Une veille active est réalisée sur les vulnérabilités liées aux supports des données et des actions correctrices sont prises en cas d'impact sur le système d'information.
Gérer les violations de données	Des incidents sont signalés. Des mesures correctrices sont parfois prises. Une notification de violation de données est parfois effectuée auprès de la CNIL.	La gestion des incidents, mise en œuvre de manière centralisée, inclut les violations de données. Des mesures correctrices sont systématiquement prises. Une communication aux personnes dont les données ont fait l'objet d'une violation pouvant engendrer un risque élevé est prévue.	Une procédure de gestion des violations de données est formalisée et mise en œuvre de manière systématique. Toutes les violations sont inscrites dans un registre dédié. Suite à une violation de données, un plan d'action est prévu afin de réduire le risque qu'elle ne se reproduise.	L'application des mesures correctives est vérifiée. Des indicateurs de suivi des violations de données sont créés et communiqués (ex. : dans le bilan annuel).	Un bilan des violations est régulièrement réalisé afin d'identifier et de mettre en œuvre des mesures permettant d'améliorer la sécurité des données. La gestion des violations de données alimente les études de risques (ex. : AIPD). Une gestion automatique des traces permet de détecter les violations de données dans les plus brefs délais.

Références

- Le règlement général sur la protection des données (RGPD)
- La loi Informatique et Libertés
- Le guide relatif à la maturité SSI, Agence nationale de la sécurité des systèmes d'information (ANSSI)
- ISO/IEC 21827 – Technologies de l'information – Techniques de sécurité – Ingénierie de sécurité système – Modèle de maturité de capacité (SSE-CMM®), Organisation internationale de normalisation (ISO)
- ISO/IEC 27001 – Technologies de l'information – Techniques de sécurité – Systèmes de management de la sécurité de l'information – Exigences, ISO
- ISO/IEC 29190 – Technologies de l'information – Techniques de sécurité – Modèle d'évaluation de capacité à la protection de la vie privée, ISO