**Modèle de maturité CNIL et Cyberattaques : 4 actions pour rassurer**

Dans un contexte post-covid très instable, face à des obligations règlementaires et des menaces cyber inédites, les organisations ont besoin de consolider leurs activités et rassurer clients, utilisateurs et investisseurs.

En quelques mois, à cause et grâce au Covid, le marché a gagné en maturité et en expérience, ce qui a conduit les acteurs de la conformité et les régulateurs, dont la CNIL avec son modèle de maturité publié le 9 septembre 2021, à mettre à disposition des organisations, des outils qui permettent aux organisations d’engager des actions concrètes et pragmatiques leur permettant de faire face.

Dans ce contexte, plusieurs constats permettent de comprendre l’urgence d’agir :

* Depuis le Covid, les services d’audit interne multiplient leurs interventions et déplorent que les entreprises sous-traitantes ne respectent pas la réglementation et ne disposent pas de mesures de sécurité susceptibles de protéger leurs clients.
* La concurrence entre entreprises sous-traitantes n’a jamais été aussi tendue, ce qui autorise les acheteurs à augmenter leur niveau d’exigence en imposant des demandes qui paraissaient déraisonnables il y a encore quelques mois.
* Bon nombre de sinistres cybers analysés par les compagnies d’assurances ont fait apparaître des lacunes en matière de conformité et de sécurité qu’elles refusent désormais de couvrir.

Nous avons identifié ainsi quatre actions prioritaires pour assurer et rassurer efficacement clients, utilisateurs et investisseurs :

1. Initier une nouvelle auto-évaluation avec le modèle de maturité publié par la CNIL le 9 septembre 2021
2. Mettre en place des indicateurs objectifs en matière de sécurité, en s’appuyant sur des outils qui permettent de disposer d’une notation sécurité par une tierce partie et notamment des outils tels que SecurityScorecard ou Bitsight.
3. Mettre en place et faire vivre un dossier de conformité solide adapté aux spécificités de l’entreprise, incluant les 61 mesures du modèle de la CNIL dont on extraira les éléments clés pour mettre à la disposition des équipes commerciales une base de connaissance les aidant à répondre aux clients et aux prospects et ainsi ne pas perdre de marchés.
4. Mixer des compétences internes (savoir-faire métier) et externes (expertise RGPD, cybersécurité) pour garantir une réelle expertise (capacité à se protéger et protéger ses partenaires contre les attaques malveillantes) et être capable de faire face à la variabilité de la demande.

**Première action :**

**Initier une nouvelle auto-évaluation avec le modèle de maturité publié par la CNIL le 9 septembre 2021**

Le 9 septembre 2021, la CNIL a partagé ses premières réflexions sur la réalisation d’un modèle de maturité en gestion de la protection des données et a mis en ligne sur son site une [première version de son modèle d’autoévaluation](https://www.cnil.fr/sites/default/files/atoms/files/autoevaluation_de_maturite_en_gestion_de_la_protection_des_donnees.pdf). Le projet de modèle décrit « 8 activités types liées à la protection des données en 5 niveaux de maturité ».

Nous avons testé ce modèle, dénommé “méthode de maturité” auprès de différentes entreprises clientes. Les retours des dirigeants opérationnels sont étonnamment positifs compte tenu du caractère réglementaire austère de la conformité RGPD. Ce modèle est un bel exemple de que peut produire l’intelligence juridique, puisqu’il va non seulement permettre aux Directions Juridiques et aux Délégués à la Protection des Données (DPO) de structurer les Dossiers de Conformité, mais aussi de sécuriser et d’éclairer les stratégies et les prises de décision. La méthode propose six niveaux de maturité de manière générique :

1. **Pratique inexistante ou incomplète**
2. **Pratique informelle** (quelques actions isolées)
3. **Pratique répétable et suivie** (des actions reproductibles)
4. **Processus défini** (standardisation des pratiques)
5. **Processus contrôlé** (mesure quantitative et correction des défauts)
6. **Processus continuellement optimisé** (amélioration continue)

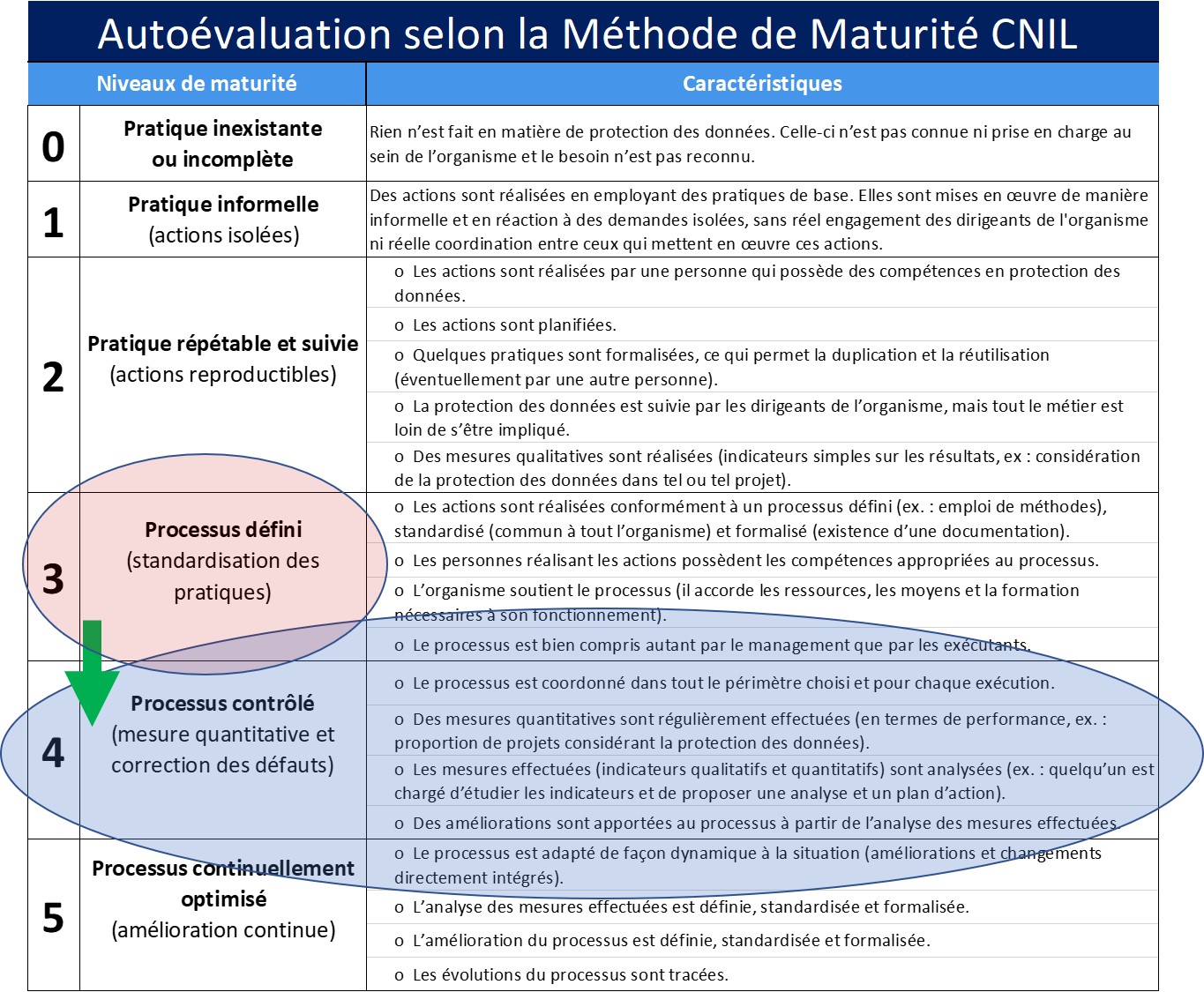
Chaque niveau évalue la manière dont un organisme conçoit, met en œuvre, contrôle, maintient et assure le suivi d’une activité, quel que soit cette activité. L’atteinte d’un niveau supérieur suppose d’avoir déjà atteint le niveau précédent.

Si le niveau 3 peut être facilement atteint, les niveaux supérieurs vont nécessiter implication et récurrence des actions.

Pour mieux appréhender l’intérêt opérationnel de ce modèle, nous avons réalisé une évaluation de maturité avec les responsables de traitement de différentes entreprises dans lesquelles nous intervenons comme DPO externalisé. Nous avons passé en revue les 61 mesures de la méthode niveau par niveau. Nous les avons interrogés ensuite sur le niveau qui leur apparaissait raisonnable compte tenu des spécificités de leurs entreprises (missions, domaine d’activité). Cette démarche a permis à chacune d’entre elles d’apprécier le chemin parcouru et de lister les actions à mettre en œuvre pour atteindre le niveau de maturité escompté.

Leurs commentaires sont les suivants :

* *“Il est précieux pour les dirigeants de l’entreprise de s’appuyer sur un référentiel objectif émis par la CNIL”*, l’un d’entre eux nous a demandé de venir présenter nos conclusions à son prochain conseil d’administration, même si comme l’indique la CNIL : “*ce modèle est un projet qui fait état des réflexions de la CNIL sur la maturité. Il ouvre la voie à de nombreux usages et outils pour l'accompagnement des organismes »*. *« En citant des exemples concrets, il facilite la formalisation d’un plan d’action pour combler les écarts constatés entre l'existant et la cible”.*
* *“Il permet de mieux cerner les attentes du régulateur et d’être prêt en cas de contrôle ou de réponse à fournir à un client”.* En rappelant que le RGPD, c’est aussi assurer la conformité juridique des traitements, former et sensibiliser, traiter les demandes des usagers internes et externes, gérer les risques de sécurité et gérer les violations de données, la CNIL fournit ici un outil d’analyse pragmatique, comme elle l’indique dans son communiqué du 9 septembre 2021 : « *cette méthodologie n’a pas pour objet d’assurer de fait la conformité. C’est un outil d’aide à l’analyse qui pourra contribuer à mettre en place des conditions favorables pour l’organisation des actions requises et les rendre pérennes, dans la logique de responsabilisation des acteurs (accountability). »*
* *“Il est une incitation au progrès, l’entreprise doit fournir à ses clients des services lui permettant de revendiquer a minima un niveau de maturité 4* ***processus contrôlé****.”* L’entreprise qui veut développer son activité avec des clients renommés, comme tiers de confiance ou sous-traitant (article 28 du RGPD) en fournissant des services et solutions en mode SAAS, ne peut plus se contenter d’un niveau de maturité 3 **processus défini** (niveau de mature 3).



L’utilisation de cette méthode est utile dans le contexte d’incertitude qui est le nôtre, même si : *« ce modèle est un projet qui fait état des réflexions de la CNIL sur la maturité. Il ouvre la voie à de nombreux usages et outils pour l'accompagnement des organismes. Il permet aux organismes d’évaluer leur propre niveau de maturité et de déterminer comment améliorer leur gestion de la protection des données. Un plan d’action pour combler les écarts constatés entre la pratique et le niveau adéquat ciblé par chaque organisme peut ainsi être élaboré sur cette base.*

Le DPO et la Direction Juridique vont donc enfin disposer de l’outil d’animation pour l’exercice de ses missions qui leur manquait. Cet outil va leur permettre de renforcer crédibilité et valeur ajoutée auprès de responsables de traitement sur les huit activités liées à la protection des données que l'on retrouve dans tout organisme :

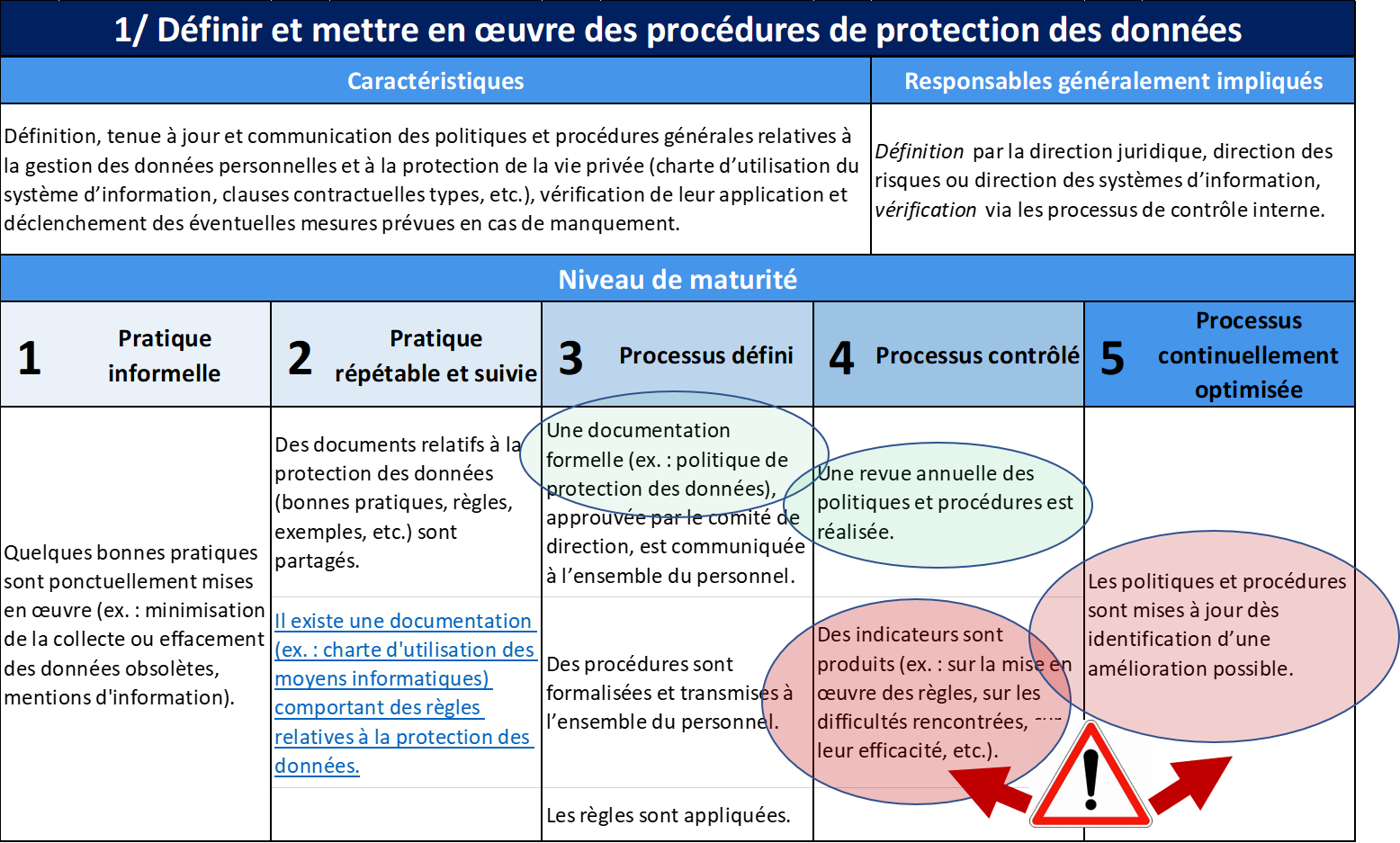
1. Définir et mettre en œuvre des procédures de protection des données
2. Piloter la gouvernance de la protection des données
3. Recenser et tenir à jour la liste des traitements
4. Assurer la conformité juridique des traitements
5. Former et sensibiliser
6. Traiter les demandes des usagers internes et externes
7. Gérer les risques de sécurité
8. Gérer les violations de données

Pour chacune de ces activités sont prédéfinis les principales caractéristiques, les responsables généralement impliqués, ainsi que quelques exemples concrets de réalisation permettant de déterminer le niveau de maturité par activité.

1. **Définir et mettre en œuvre des procédures de protection des données**

Si la définition et la rédaction des procédures est à la portée de tous, la vérification de leur application et le déclenchement des éventuelles mesures prévues en cas de manquement sont plus difficiles à mettre en œuvre.

Parmi les principes prioritaires, certains se révèlent assez simples à mettre en place (documentation formelle, revue annuelle) alors que d’autres apparaissent sur le terrain plus complexes à formaliser et à maintenir durablement. On évoquera notamment les indicateurs objectifs qui doivent être formalisées ou encore la mise à jour de la documentation dès l’identification d’une amélioration possible .



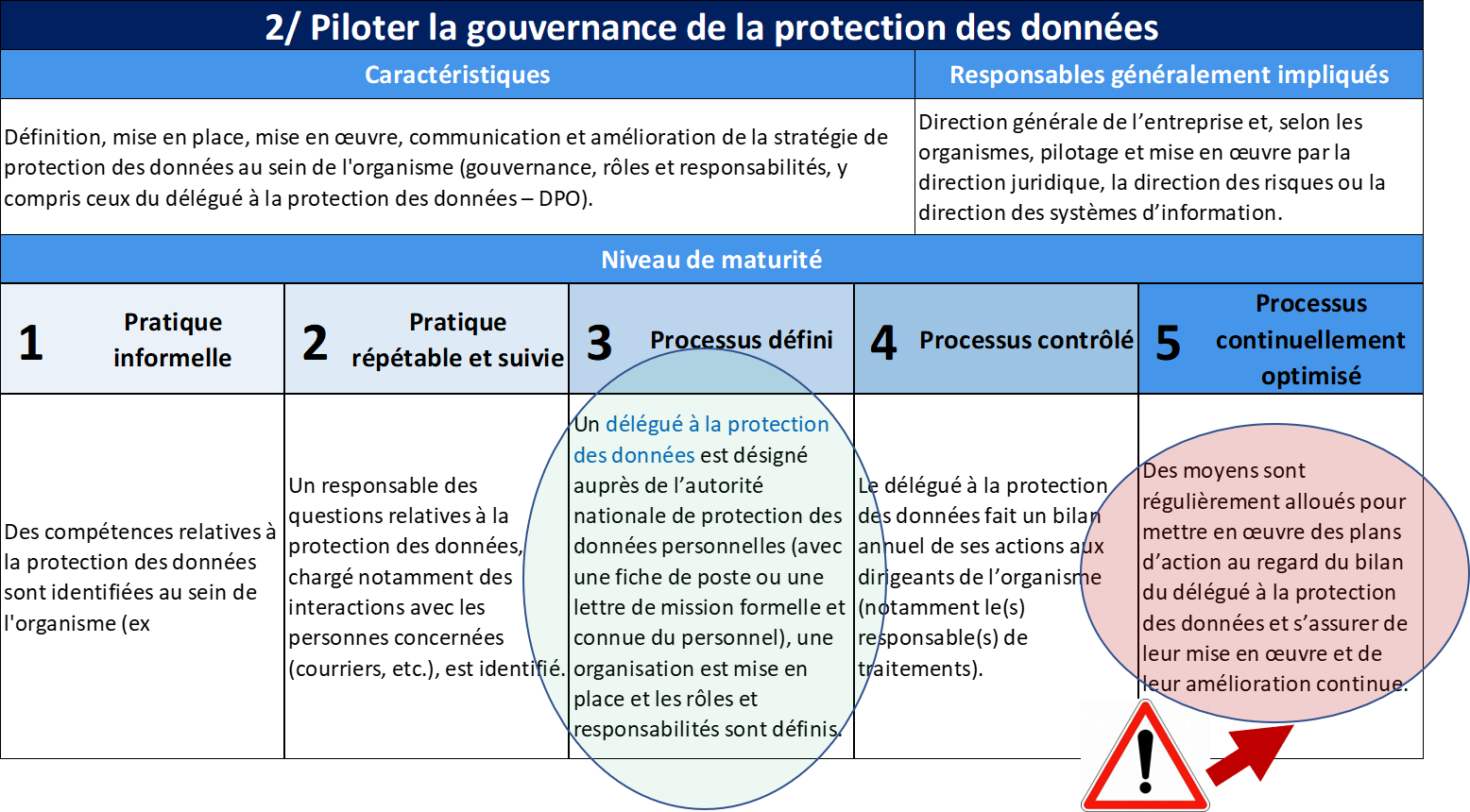
Il ne s’agit pas simplement de documenter, il faut réussir à faire vivre la conformité. C’est ce que nous nous efforçons de faire depuis l’entrée en application du RGPD en proposant à nos clients de regrouper la documentation formelle dans un dossier de conformité, facilement accessible par les personnes habilitées désignées par l’organisation et de faire vivre ce dossier de conformité par des comités RGPD mensuel.

Néanmoins, suite à la publication de ce modèle de maturité, comme cela sera abordé dans la troisième action, l’évolution de la configuration des dossiers de conformité s’imposait. Il convenait d’y intégrer au plus vite les compléments pertinents extraits du modèle de maturité proposé par la CNIL.

1. **Piloter la gouvernance de la protection des données**

Un pilotage de la gouvernance sous-entend qu’il doit impliquer les différents responsables de l’organisation autant faire se peut.

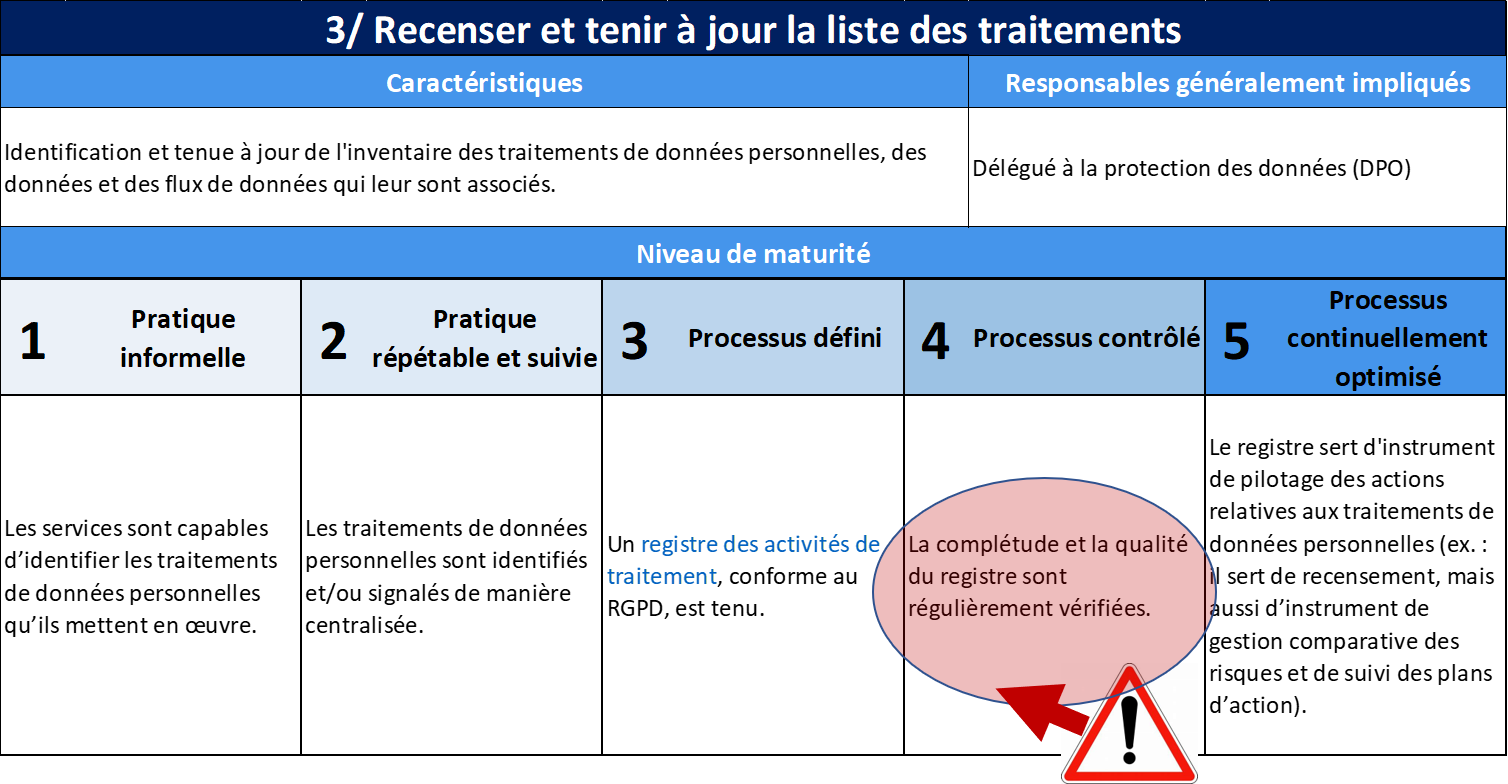
Ce pilotage est de manière générale assuré par le DPO, ces caractéristiques sont la mise en place, la mise en œuvre, la communication et l’amélioration de la stratégie de protection des données au sein de l'organisme (gouvernance, rôles et responsabilités, y compris ceux du délégué à la protection des données – DPO).

Un bon pilotage de la gouvernance se veut efficace. Il permet l’existence de processus à jour optimisés ou a minima contrôlés. L’évaluation de chacune des activités est l’occasion d’un échange pédagogique avec le dirigeant et son équipe qui va permettre aux uns et aux autres de prendre connaissance et conscience des sujets de conformité identifiés par le DPO.

Lors des périodes de négociation budgétaire avec la direction, la crédibilité du DPO est essentielle, car même si celui-ci peut s’appuyer sur des collaborateurs juniors, l’expérience est utile pour convaincre.

1. **Recenser et tenir à jour la liste des traitements**

Comme l’indique la CNIL, le registre sert d'instrument de pilotage des actions relatives aux traitements de données personnelles. A titre d’exemple, il permet de cartographier les données mais se révèle être aussi un instrument précieux de gestion comparative des risques et de suivi des plans d’action.

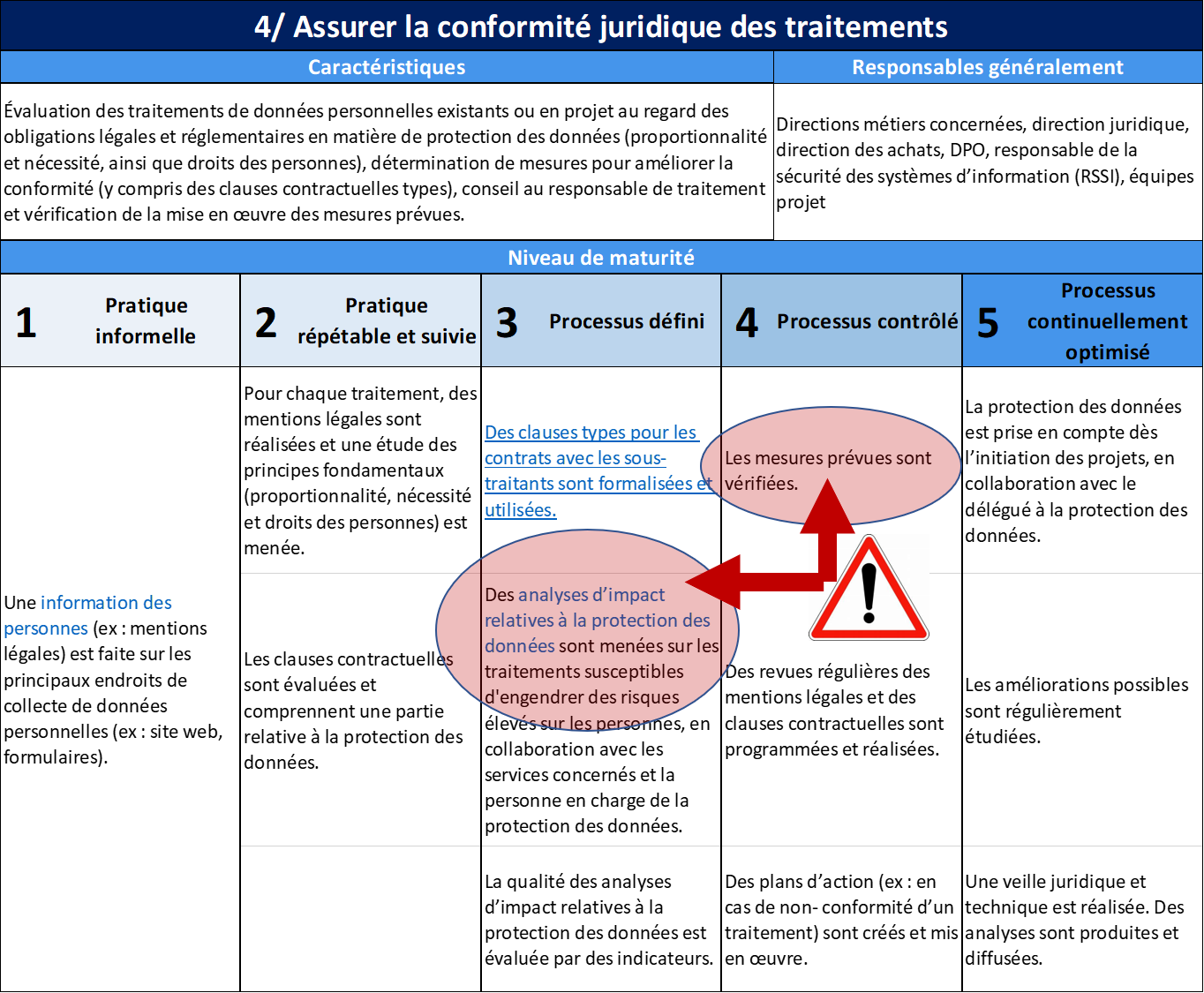


Qu’il ait été généré par un outil spécialisé qui a souvent le gros inconvénient de gérer une multitude d’informations inutiles au regard des obligations règlementaires ou à partir du modèle Excel proposé auparavant par la CNIL, un registre de traitement est trop souvent illisible et difficile à actualiser. Dans ce contexte, le recours au [registre publié par la CNIL en décembre 2020](https://www.cnil.fr/sites/default/files/atoms/files/registre-rgpd-cnil_dec-2020.pdf), plus littéraire et plus lisible, devient incontournable.

1. **Assurer la conformité juridique des traitements**

Certains ne l’ont pas encore intégré, mais la protection des données doit non seulement être prise en compte dès l’initiation des projets (« by design »), en collaboration avec le DPO, mais le délai de grâce pour la mise en conformité des traitements existants est terminé.

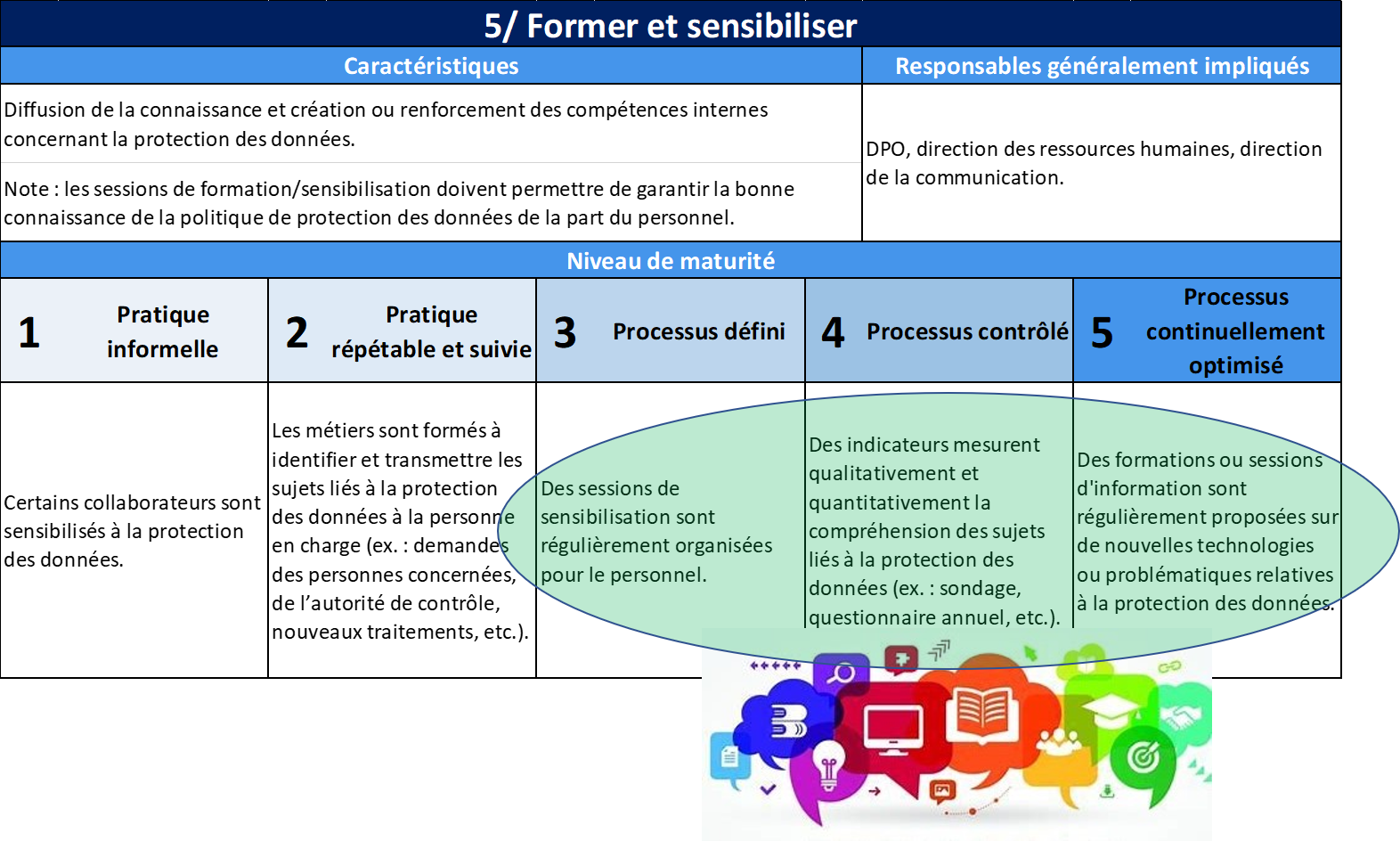
L'AIPD (ou PIA en anglais) est un outil qui permet de construire un traitement conforme au RGPD et respectueux de la vie privée. Elle concerne les traitements de données personnelles qui sont susceptibles d'engendrer un risque élevé pour les droits et libertés des personnes concernées. Si en mai 2018, l’AIPD n’était obligatoire que pour les nouveaux traitements de données à caractère personnelle respectant certains critères, l’obligation est étendue depuis 2021 à l’ensemble des traitements d’une organisation.



Pour beaucoup de dirigeants, l’analyse d’impact (AIPD) est un sujet de friction et de coûts difficile à accepter. Les ressources internes de l’entreprise n’ont pas l’habitude et la pratique de l’exercice. Il est souvent nécessaire de mandater un prestataire et/ou un avocat pour mener à bien l’opération puis prévoir un budget et des ressources pour la mise en œuvre des mesures correctives qui accompagnent la démarche.

1. **Former et sensibiliser**

C’est un sujet simple qui se révèle plus complexe qu’on ne pourrait l’imaginer de prime abord si l’on veut le faire vivre et le rendre efficace tout en s’assurant de la bonne implication des équipes.



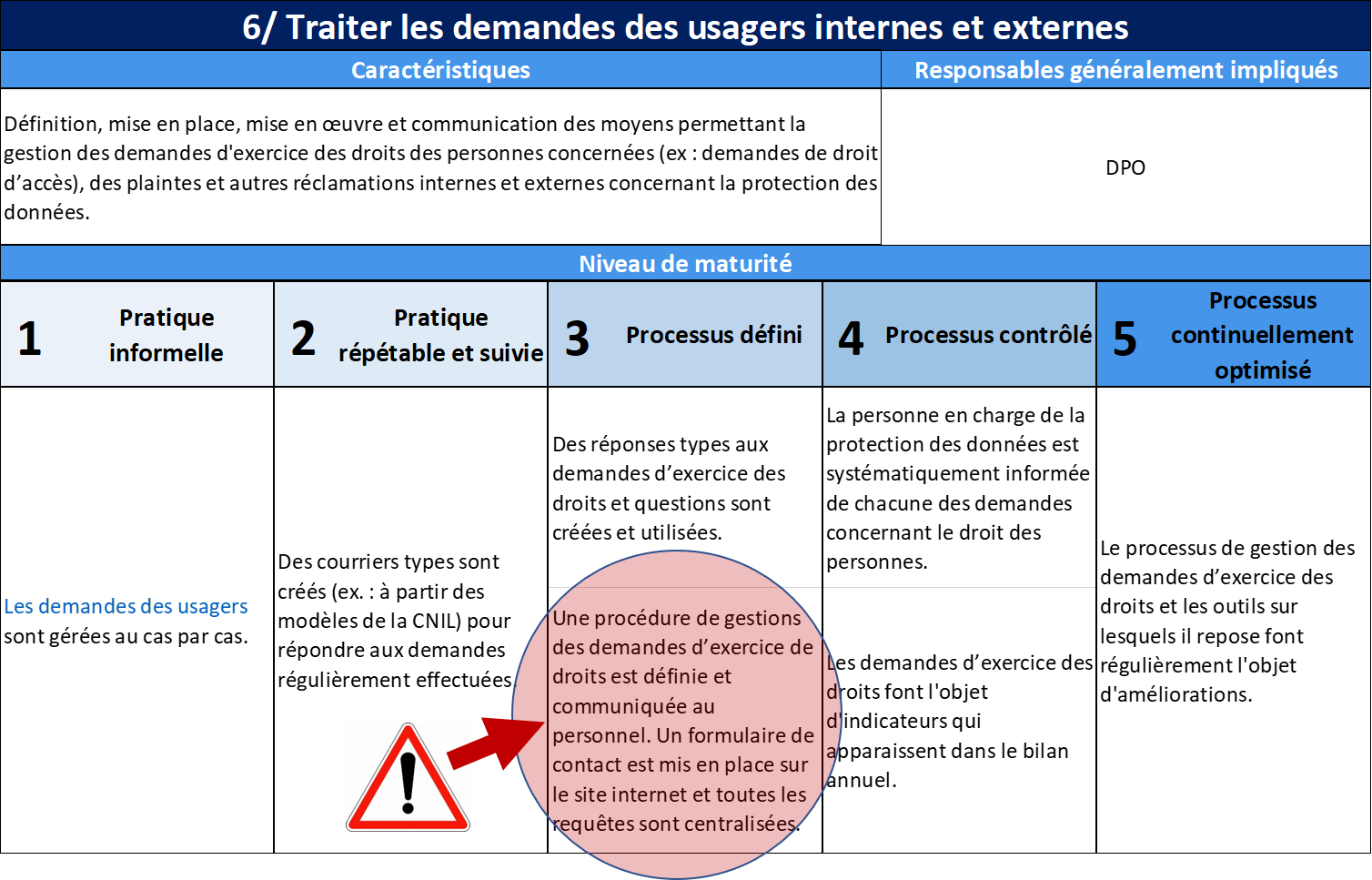
En effet, la diffusion de la connaissance, la création ou le renforcement des compétences internes concernant la protection des données se révèlent souvent peu attractifs pour les collaborateurs.

Le succès de formations ou sessions d'information sur de nouvelles technologies ou problématiques d’actualité ou opérationnelles relatives à la protection des données sera conditionnée à la qualité des supports utilisés ou le caractère communiquant du formateur.

1. **Traiter les demandes des usagers internes et externes**

La plupart des sanctions rendues par la CNIL depuis l’entrée en application du RGPD résultent de mauvaises gestions par les organisations 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.

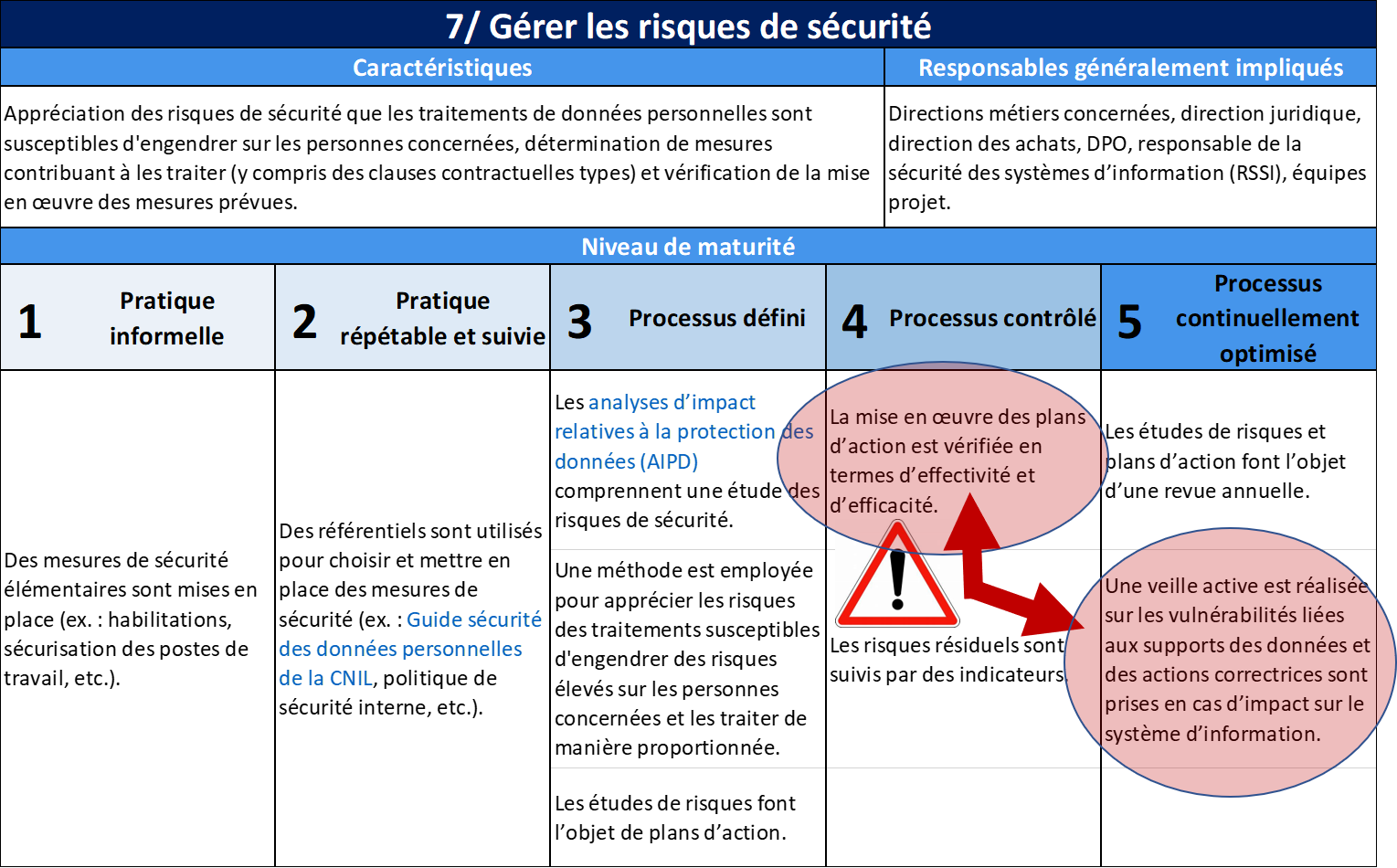
Ce fut notamment le cas pour la décision rendue à l’encontre de Carrefour le 18 novembre 2020, dans laquelle l’autorité identifiait un retard chronique dans le traitement des demandes d’exercice de droits, alors même que l’article 12 du RGPD prévoit des délais ne pouvant excéder trois mois. La récurrence des retards de traitement résulte d’un manque d’anticipation de l’augmentation des demandes post-RGPD.



Les demandes d’exercice de droits non traitées dérivent souvent en plainte à l’attention de la CNIL, qui si elles sont répétées, incite la CNIL à se saisir du sujet et à engager les investigations et enquêtes adéquates.

1. **Gérer les risques de sécurité**

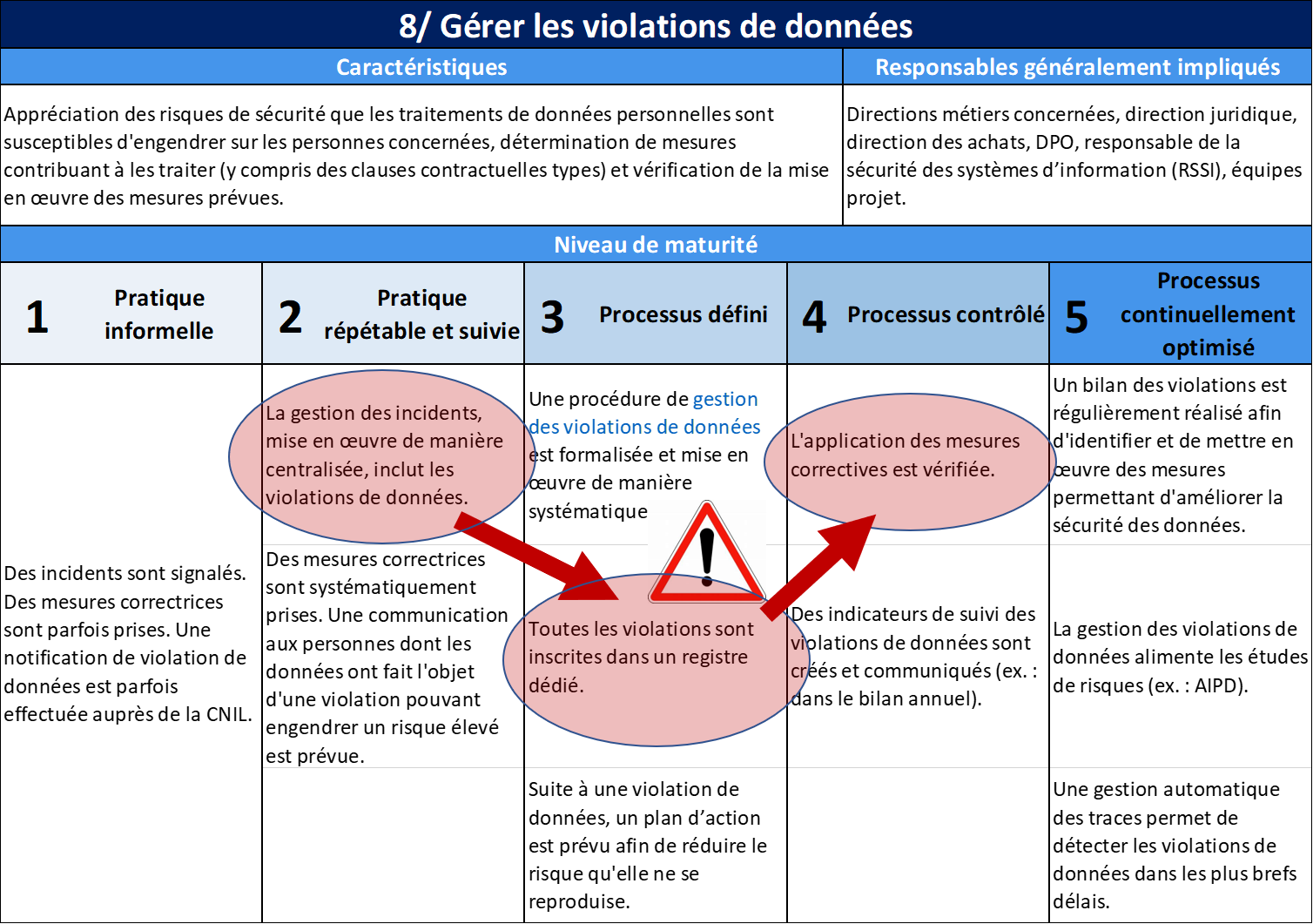
Bon nombre de sinistres cybers analysés par les compagnies d’assurances ont fait apparaître des lacunes en matière de conformité et de sécurité qu’elles refusent désormais de couvrir. L’appréciation des risques de sécurité que les traitements de données personnelles sont susceptibles d'engendrer sur les personnes concernées, la détermination de mesures contribuant à les traiter (y compris des clauses contractuelles types) et la vérification de la mise en œuvre des mesures prévues sont perfectibles dans une grande majorité d’organisations, qui, face à l’apparente complexité du sujet, font souvent part d’un renoncement inquiétant.



Comme nous le verrons dans la seconde action proposée, la mise en place des indicateurs objectifs en matière de sécurité, en s’appuyant sur des outils qui permettent de disposer d’une **notation sécurité par une tierce partie** et notamment des outils tels que SecurityScorecard ou Bitsight devient indispensable et permet de mettre en place une veille active sur les vulnérabilités liées aux supports des données et les actions correctives appropriées.

1. **Gérer les violations de données**

Cette dernière activité est la suite logique de la précédente. L’appréciation des risques de sécurité que les traitements de données personnelles sont susceptibles d'engendrer sur les personnes concernées, la détermination de mesures contribuant à les traiter (y compris des clauses contractuelles types) et vérification de la mise en œuvre des mesures prévues se révèlent ardues, car elle nécessite une capacité de réactivité au sein d’organisations qui sont souvent dépassées par la complexité techniques et opérationnelles dans la résolutions de ce type de problèmes pour lesquels elles ne disposent bien souvent pas des ressources internes habituées au traitement de ce type de situation.



Cette activité est souvent la moins maitrisée dans les organisations. Il est rare de la voir intégrée dans un process de gestion des incidents alors qu’une telle disposition autoriserait une bien meilleure anticipation des actions à mener.

Comme expliqué dans notre quatrième action, le responsable de traitement, pour peu qu’il souhaite développer son activité avec des clients renommés comme sous-traitant (article 28 du RGPD) en fournissant des services et solutions en mode SAAS, ne peut plus se contenter d’un niveau de maturité 3 « **processus défini »** (niveau de mature 3). Il est dans l’obligation de fournir à ses clients des services lui permettant de revendiquer un niveau de maturité 4 « **processus contrôlé** » plus facile à maintenir dans le temps avec des ressources externes et modulables.

**Deuxième action :**

**Mettre en place des indicateurs objectifs en matière de sécurité, en s’appuyant sur des outils qui permettent de disposer d’une notation par un tiers et notamment des outils tels que SecurityScorecard ou Bitsight.**

La CNIL souligne dans son modèle de maturité la nécessité de mettre en place des indicateurs objectifs de suivi de l’évolution du projet RGPD. La gestion des risques de sécurité ne s’improvise pas.

Depuis 2018, la cybermenace croît de manière exponentielle, avec un niveau maximum atteint au cours d'une année 2020 marquée par le Covid-19. "Le nombre de victimes a ainsi été multiplié par quatre en un an", rapportent l'Agence nationale de la sécurité des systèmes d'information (Anssi) et son homologue allemand, le BSI. Mais le GIP relève aussi une baisse conséquente des appels à l’aide de particuliers : 491 en 2020 contre 2 972 l’année précédente. Une évolution symptomatique de la réorientation des cyber délinquants vers les cibles les plus lucratives potentielles.

La montée des ransomwares et d'autres méthodes d'extorsion ont permis à ces attaques d'être menées à grande échelle et sans coûts importants. Alors que la cyberéconomie s'épanouit, les occasions de criminalité augmentent et les chances de se faire prendre s’amenuisent. *« La cybercriminalité offre une opportunité à haut rendement et à faible risque. »* (Aatish Pattni, Link11).

Les chiffres du GIP Acyma, qui a en charge le portail Cybermalveillance.gouv.fr, sont encore plus inquiétants. Jérôme Notin, directeur général du GIP, fait ainsi état de 159 collectivités touchées en 2020 contre 103 en 2019, et de 837 entreprises, contre 667.

La densité de l’actualité sur ce sujet au cours du mois estival d’août 2021 confirme également la croissance continue du phénomène et la diversité des cibles :

* Les serveurs Microsoft Exchange de six ministères des Affaires étrangères et de 8 sociétés spécialisées dans l'énergie ont été infiltrés par des cybercriminels. Des données hautement sensibles auraient été volées.
* Un hacker diffuse gratuitement pour la promotion de son black market un fichier contenant près d'un million de cartes bancaires. Au total, 40 000 Français seraient concernés par cette fuite
* Dans la nuit du samedi au dimanche 1er août 2021, une cyberattaque, supposément par rançongiciel, a frappé les services informatiques du Latium, une région au centre de l'Italie où se situe la ville de Rome.

Les entreprises de moins de 50% sont également directement impactées : 41 % des entreprises interrogées de 0 à 9 salariés et 44% des entreprises de 9 à 49 salariés ont déjà subi une ou plusieurs attaques ou tentatives d’attaques informatiques (données 2019).

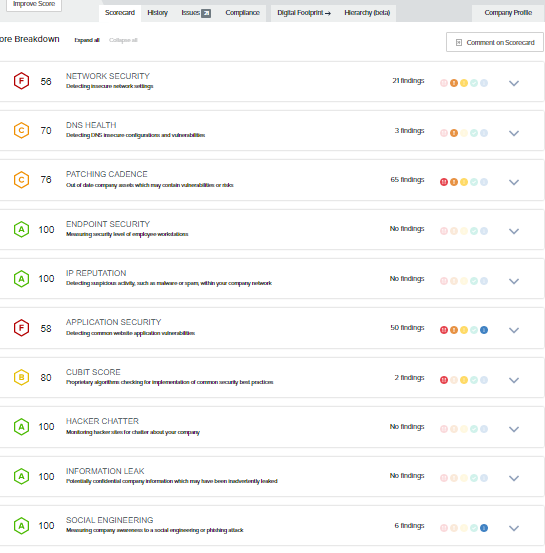
Le recours à des outils tiers objectifs devient dès lors un moyen convaincant pour démontrer son niveau de maturité en termes de cybersécurité.

Il existe plusieurs offres sur le marché telles que Frequent, Bitsight ou encore Securityscorecard. Pour rentrer plus dans l’opérationnel, nous prendrons pour exemple Sécurityscorecard qui se distingue par son ergonomie soignée et qui vient d’être désigné par le Gartner comme *Gartner Peer Insights ‘Voice of the Customer’: IT Vendor Risk Management Tools* . Bon nombre de grandes banques et de compagnies d’assurance sont actionnaires de cette solution et l’utilisent pour évaluer les risques associés aux partenaires ou fournisseurs tiers ou surveiller leur propre infrastructure Internet accessible au public pour détecter les risques et les vulnérabilités.

Une image contenant texte

Description générée automatiquement

Le tableau de bord principal qui apparaît en premier lieu permet de disposer d’une évaluation globale suivie d’une évaluation plus détaillée du nom de domaine analysé. Les niveaux d’évaluation sont A, B, C, D et F.



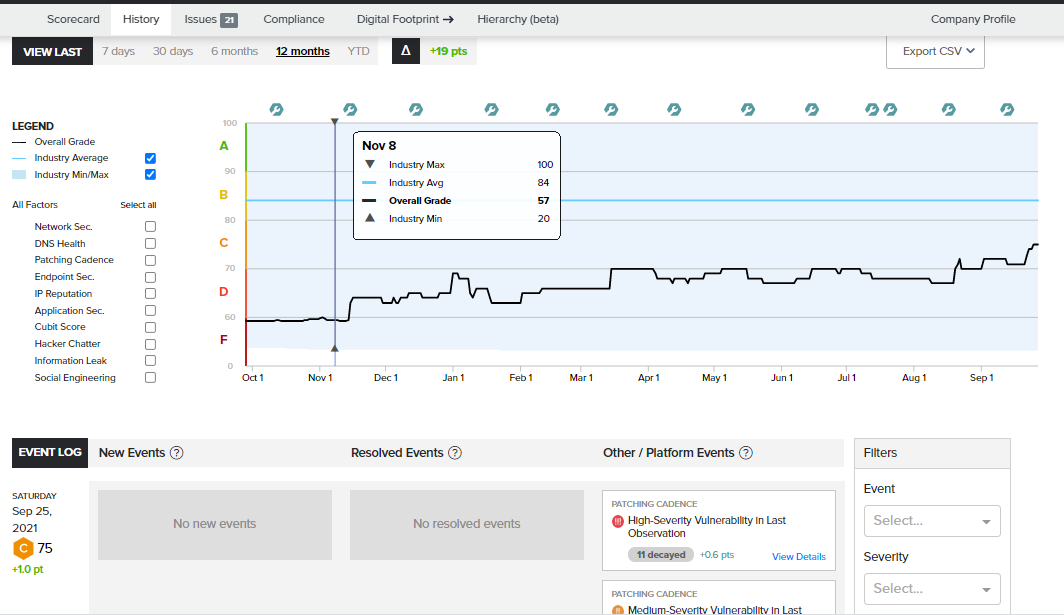
Les compagnies d’assurance jugent qu’une entreprise est viable si elle a une note globale de A ou B. Au-delà, elle refusera dans certains cas de contracter avec elle (client ou fournisseur).

Un tableau des anomalies détectées pour chaque domaine de vulnérabilité est disponible et oriente de manière détaillée le développeur ou le responsable des infrastructures dans la résolution de la vulnérabilité. Le niveau de sévérité de chaque anomalie permet de prioriser les actions correctives.

Une image contenant texte

Description générée automatiquement

Au fur et à mesure que les anomalies sont corrigées, il est possible d’en informer la plateforme qui effectuera à intervalles réguliers un contrôle puis réévaluera l’ensemble du périmètre. Une évolution dans le temps peut être consultée pour apprécier les résultats des actions menées.



Si la conformité ISO27001 est un bon outil pour crédibiliser le niveau de sécurité de son entreprise, elle se révèle lourde et complexe à mettre en œuvre pour les PME. L’autre alternative est donc l’utilisation de ce type d’outil qui se révèle particulièrement utile lorsqu’il s’agit de démarrer un projet de cybersécurité. Il sert de fil d’Ariane pour le Chef de projet qui peut aborder son plan d’action en tenant compte du risque. Il est aisé ensuite de démontrer auprès d’un prospect ou d’un investisseur le niveau d’invulnérabilité atteint.

**Troisième action :**

**Mettre en place et faire vivre un dossier de conformité solide adapté aux spécificités de l’entreprise dont on extraira les éléments clés pour mettre à la disposition des équipes commerciales une base de connaissance les aidant à répondre aux clients et aux prospects et ainsi ne pas perdre de marchés.**

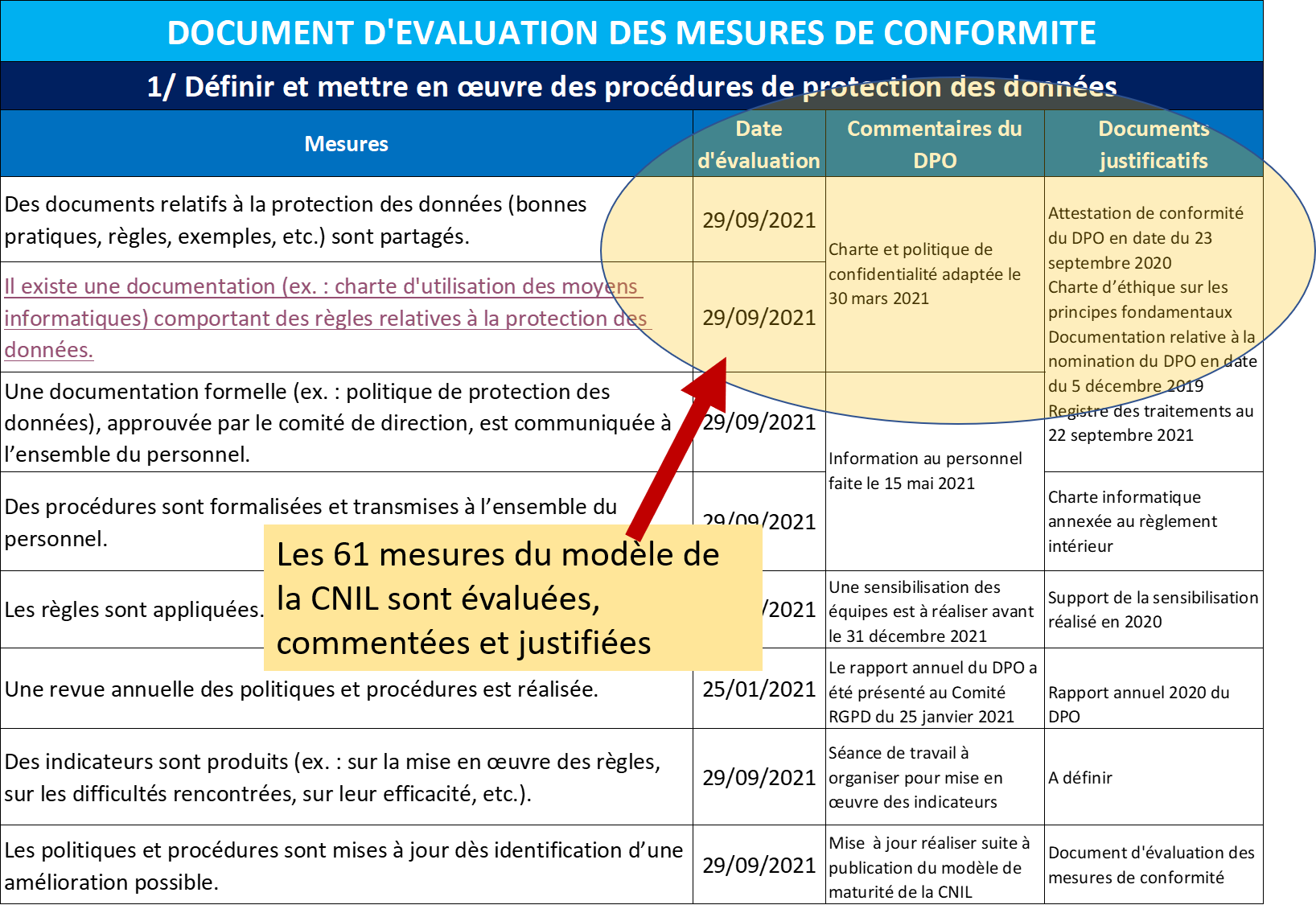
La mise en conformité et la gestion quotidienne du RGPD imposent à l’organisation le déploiement des mesures appropriées (techniques, organisationnelles, contractuelles, etc.) et d’être en mesure de démontrer sa conformité à tout moment. Cette démonstration se base notamment sur la production d’une documentation exhaustive et détaillée, décrivant l’ensemble des procédures et des bonnes pratiques appliquées par l’organisation en matière de données personnelles. Les éléments documentaires réglementaires ainsi produits sont regroupés dans un dossier de conformité, accessible par les personnes habilitées désignées par l’organisation.

Selon le contexte (nature et volume des données traitées notamment), les dossiers de conformité produits comportaient jusqu’à présent différents documents, organisés autour de cinq thèmes :

* Les fondamentaux de la conformité
* Transparence et information des personnes
* Sécurité, intégrité et confidentialité
* Aspects contractuels : Contrôle et audit de l’efficacité des mesures déployées

La publication le 9 septembre 2021 du modèle de maturité de la CNIL a incité à compléter les dossiers de conformité pour tenir compte du modèle de maturité proposé par la CNIL en y ajoutant un document d’évaluation.

La nouvelle version de l’outil d’évaluation reprend les 61 mesures listées par la CNIL dans sa méthode sans en préciser le niveau de maturité, mais en partant du principe que chaque mesure complète l’autre et qu’une mesure de base peut cohabiter avec une mesure de contrôle ou d’optimisation, car comme vu précédemment des mesures de niveau 3 peuvent être plus importantes que des mesures de niveau 5.



Pour chacune des mesures, le document mentionne une date d’évaluation de la mesure, ainsi que les éventuels commentaires du DPO.

Les liens hypertextes présents dans ce dossier permettent d’accéder aux documents justificatifs de l’effectivité de la mesure et aux équipes opérationnelles de disposer instantanément des éléments clés dans la base de connaissance leur permettant de répondre aux clients et aux prospects et ainsi ne pas perdre de marchés.

**Quatrième action :**

**Mixer des compétences internes (savoir-faire métier) et externes (expertise RGPD, cybersécurité) pour garantir une réelle expertise (capacité à se protéger et protéger ses partenaires contre les attaques malveillantes) et être capable de faire face à la variabilité de la demande.**

Les entreprises du CAC40 et du SBF120 deviennent de plus en plus fébriles face à l’explosion de la cybercriminalité. La conformité RGPD et la certification ISO27001/2 ou encore le « zero trust » leur apparaissent soudain comme des avantages différenciants crédibles. Les questionnaires fournisseurs RGPD et sécurité s’étoffent et s’accompagnent le plus souvent d’une soutenance orale. Un fournisseur n’étant pas en mesure de démontrer son niveau de sécurisation a toutes les chances de se voir fermer la porte au nez.

Les PME et ETI se voient soudainement dans l’obligation d’intégrer ces nouvelles contraintes à marche forcée pour ne pas pénaliser leur activité commerciale.

La mise en conformité RGPD et la cybersécurité sont des domaines spécifiques pour lesquels il faut savoir placer adroitement le curseur entre internalisation et externalisation.

Avant toute chose, une attention toute particulière doit être accordée au savoir-faire métier et à la stratégie de l’organisation. Étant donné sa connaissance de la culture d’entreprise et l’expérience acquise dans son cœur de métier, seul un collaborateur interne sera à même de préserver ses valeurs intrinsèques.

Il convient ensuite d’identifier les différentes expertises nécessaires à la gestion de la conformité RGPD et de la cybersécurité. Elles peuvent être regroupées en trois catégories : organisationnelle, juridique et technique :

* Les savoirs organisationnels : il convient d’élaborer des procédures et des politiques, ce qui induit des connaissances en gouvernance des entreprises. Par ailleurs, il faut être en mesure de mener un audit de conformité et de proposer des mesures de réduction ou gestion des risques, de les évaluer et d’en surveiller la mise en œuvre. Un chef de projet interne doit pouvoir piloter cette activité. Il devra en revanche être épaulé par des experts spécifiques.
* Les savoirs techniques et informatiques : on doit mettre en œuvre des principes de minimisation ou d’exactitude, d’efficacité et d’intégrité des données et pouvoir exécuter des demandes de modification et d’effacement de données, ce qui impacte les systèmes et les applications de l’entreprise. Si les équipes techniques de l’entreprise doivent être en mesure d’assumer ce périmètre, des savoirs très pointus (configuration infrastructure, développement web, « privacy by design », ...) devront être sollicités. L’intervention d’une expertise technique externe présente également l’avantage de pouvoir challenger les collaborateurs internes et faire sauter quelques verrous préjudiciables à une gestion efficace.
* Les savoirs juridiques : un expert en protection juridique et règlementaire des données à caractère personnel, un Data Protection Officer (DPO) doit être associé à la démarche. Outre le RGPD, il peut conseiller l’entreprise en cas de conflit de lois. Il participe à l’élaboration des contrats avec les partenaires, peut négocier avec le DPO du partenaire les clauses de protection de données personnelles. Il a également un rôle essentiel à jouer en matière de contentieux : il est l’interlocuteur de la CNIL et il instruit les plaintes des personnes concernées.

On notera enfin que les savoirs techniques, informatiques et juridiques liés au RGPD et à la cybersécurité sont des domaines particulièrement soumis aux évolutions.

Si l’entreprise n’a pas démarré sa mise en conformité RGPD ou si l’écart d’expertise à combler est trop important, l’externalisation totale ou partielle de ces expertises peut être une option viable. Pour une entreprise de petite ou moyenne taille qui ne souhaite pas disposer d’un DPO en interne, avoir recours à des services extérieurs mutualisés est une des possibilités les plus pertinentes.

Mais une externalisation partielle présente aussi l’avantage d’accompagner le DPO interne dans une partie de ses activités, avec un partage des pratiques professionnelles à l’aune des contraintes de l’entreprise.