CYBERSECURITE ET PROTECTION DES DONNEES PERSONNELLES

–

CADRE DE GOUVERNANCE ET DISPOSITIFS

Mars 2026

SOMMAIRE

1. Objet et périmètre du document

Cette note présente le cadre de gouvernance, les principes ainsi que les principaux dispositifs mis en œuvre par le Groupe SEB en matière de cybersécurité, de sécurité de l'information et de protection des données personnelles. Elle s'inscrit en complément du Document d'Enregistrement Universel (DEU) et du Code éthique du Groupe.

Le Groupe reste engagé dans une démarche de transparence raisonnée envers ses parties prenantes, en partageant les éléments pertinents de son cadre de gouvernance et de ses dispositifs, tout en préservant l'efficacité opérationnelle de ses mesures de protection.

2. Gouvernance de cybersécurité

2.1. Une organisation dédiée

Au sein de la Direction des Systèmes d'Information (*DSI*), la Direction de la Sécurité des Systèmes d'Information (*DSSI*), dirigée par la Directrice de la Sécurité des Systèmes d'Information (ou Responsable de Sécurité des Systèmes d'Information *RSSI*), est en charge de piloter la sécurité des systèmes d'information, c'est à dire d'identifier et d'évaluer les risques et de définir la gouvernance, mobiliser les ressources et mettre en œuvre l'ensemble des politiques, process et systèmes permettant de répondre de manière satisfaisante aux risques identifiés.

Elle s'appuie donc sur une analyse des risques des systèmes d'information, remises à jour annuellement. L'ensemble des actions est priorisé en fonction des risques de sécurité des systèmes d'informations afin de concentrer les moyens de prévention, de détection et de remédiation sur les risques les plus significatifs.

Elle est organisée selon quatre grands piliers :

- Gestion de la stratégie et gouvernance cyber
- Protection des utilisateurs
- Protection des données
- Protection des actifs numériques et techniques

Ces différents piliers permettent de soutenir l'ensemble du système d'information pour assurer son maintien en condition de sécurité.

La DSSI s'assure de la conformité aux différentes législations et obligations réglementaires en vigueur en fonction de la territorialité. Elle agit en deuxième ligne de défense en s'assurant du respect des politiques qu'elle édite et en assurant un suivi régulier de l'application des politiques et de l'efficacité des dispositifs de contrôle mis en œuvre au sein du Groupe.

La DSSI est composée d'une équipe gouvernance et d'une équipe de sécurité opérationnelle.

L'équipe de sécurité opérationnelle répond aux besoins de sécurité exprimés par l'équipe gouvernance en sélectionnant un ensemble de partenaires pour être accompagné sur les sujets de sécurité informatique et s'équiper d'équipements et de solutions reconnus pour la protection et la détection d'incidents. Elle comprend en son sein une sous-organisation dédiée afin d'assurer la détection et la réponse aux évènements de sécurité (*Security Operations Center, SOC, et Computer Emergency Response Team, CERT*).

2.2. Cadre de référence et mission

La DSSI a pour mission principale de définir la stratégie et les évolutions du dispositif de sécurité déjà mis en place afin de répondre aux enjeux de la sécurité des systèmes d'information de l'organisation. Les propositions d'évolution du dispositif s'appuient sur la stratégie, la cartographie des risques et la conformité réglementaire. Le dispositif de sécurité est structuré en cohérence avec les recommandations d'autorités de référence telles que *le National Institute of Standards and Technology* (NIST) ou *l'International Organization for Standardization* (ISO), et avec les standards applicables au Groupe. Le NIST *Cybersecurity Framework* s'articule selon six domaines :

- La gouvernance
- L'identification
- La protection
- La détection
- La réponse
- La reprise d'activité, qui inclut les aspects de résilience et de gestion de crise

Cette approche s'appuie sur les deux principes que sont la **défense en profondeur** (*defense in depth)* et la **sécurité dès la conception** (*security by design).*

Elle s'applique à trois périmètres que sont l'IT (*Information Technology*), l'OT (*Operational Technology*) et l'IoT (*Internet of Things*) pour les produits connectés du Groupe SEB.

La direction promeut les valeurs suivantes dans son action :

- **Collaboration :** la sécurité doit être incarnée par tous les utilisateurs des systèmes d'information du groupe SEB, en particulier les équipes IT,
- **Transparence :** Les règles doivent être connues pour être appliquées, et
- **Simplicité :** les règles doivent être simples pour être mises en œuvre.

La vision de la direction cybersécurité est d'établir une sécurité des systèmes d'information juste et agile, qui soutienne l'innovation et l'évolution du Groupe SEB.

2.3. Gouvernance et supervision

Le comité exécutif de la Direction des Systèmes d'Information (*Comex*) est informé mensuellement du statut de la cybersécurité au sein du Groupe. Une présentation détaillée est faite au Comex selon une fréquence au moins semestrielle. Les enjeux de cybersécurité sont intégrés à la cartographie des risques du Groupe et font l'objet d'un suivi dans le cadre des dispositifs de contrôle interne et de gestion des risques.

Concernant les exigences liées à la protection des données personnelles, la RSSI travaille en lien avec la Responsable de la Protection des Données Personnelles (DPO), la Direction Juridique, la Direction de la Conformité et la Direction de l'Administration du personnel. Cette articulation entre les fonctions DSI, DSSI, DPO, Juridique, Conformité et Audit interne permet d'assurer une couverture cohérente des enjeux de cybersécurité, de sécurité de l'information et de protection des données personnelles.

La DSSI travaille également en collaboration avec le service d'Audit Interne pour valider annuellement les contrôles liés à la sécurité et leur plan de revue.

2.4. Sensibilisation et culture cyber

La cybersécurité est l'affaire de tous, ainsi tous les nouveaux arrivants au sein du Groupe sont sensibilisés aux enjeux de la cybersécurité à travers un kit de bienvenue édité en français et en anglais. L'ensemble des collaborateurs est également informé par mail de nouveaux risques conjoncturels, qu'ils proviennent de l'intérieur du Groupe, de ses partenaires, ou de son environnement.

La direction de la sécurité des systèmes d'informations assure également, avec l'équipe « Learning & Development » du Groupe, des formations ciblées en fonction des métiers les plus concernés et organise annuellement plusieurs tests de phishing pour sensibiliser les salariés aux techniques toujours plus sophistiquées des hackers. Le dispositif intègre également les partenaires et sous-traitants du Groupe à la prévention des risques de sécurité des systèmes d'information.

3. Surveillance des menaces et réponse à incident

3.1. Se préparer pour mieux réagir

Dans un contexte d'accroissement des cybermenaces et des attaques informatiques dans le monde, le Groupe SEB a initié dès 2020 des plans de renforcement de la sécurité des systèmes d'information. Les capacités de détection et de réaction aux cyber-attaques ont été considérablement renforcées. Un schéma directeur sécurité a été mis en œuvre dès 2022 et a défini la trajectoire du Groupe en matière de cybersécurité jusqu'en 2026. Ce plan adressait aussi bien les systèmes IT que OT. Un nouveau plan pour couvrir la période de 2026 à 2030 est en cours d'élaboration.

De plus, les nouveaux projets font l'objet d'une stratégie de sécurité dès la conception. Pour les projets de sites internet ou d'objets connectés, des tests d'intrusion sont réalisés avant la mise en production.

Le Groupe suit attentivement les recommandations et alertes émises par les autorités et organismes de référence compétents en matière de cybersécurité afin de faire face à des modes d'attaque toujours plus perfectionnés, susceptibles d'impacter la continuité d'activité ou la confidentialité des données.

Chaque année, le Comité Exécutif du Groupe SEB et les équipes des directions Industrie, DSI et Marketing se prêtent à un exercice de gestion de crise cyber qui permet l'entraînement face aux crises potentielles et le renforcement de la collaboration entre la Direction du Groupe, les métiers, fonctions et les équipes des Systèmes Informatiques.

3.2. Un dispositif de réponse à incident dédié

Groupe SEB est doté d'un Centre de Sécurité Opérationnel ou *Security Operation Center* (*SOC*) qui permet la détection avancée des vulnérabilités et des menaces et l'identification rapide de signaux faibles afin de réagir aux cyber-attaques potentielles et d'en limiter la survenance ou les impacts.

Ce service complet est doté des ressources humaines, des outils (SIEM[1], EDR[2], etc.) et des processus qui permettent au Groupe SEB d'assurer sa capacité à détecter, analyser et contenir les incidents de sécurité dans les meilleurs délais afin d'en limiter les impacts potentiels.

En parallèle, afin d'éprouver le dispositif, des exercices dits de « *Red teaming »,* où des hackers éthiques professionnels d'une société spécialisée tentent de pénétrer les cyberdéfenses du Groupe, sont menés en coordination avec l'équipe d'Audit Interne du Groupe.

L'ensemble de ces dispositifs fait l'objet de revues et d'améliorations régulières. Les résultats des contrôles et des exercices alimentent un processus d'amélioration continue qui contribue au renforcement de la posture de sécurité du Groupe.

La direction de la sécurité des systèmes d'information encadre également la mise en œuvre et le test de plans de reprise d'activité, définit des plans de continuité d'activité avec les métiers et a désigné un processus de gestion de crise cyber pour Groupe SEB.

[1] *Security Information and Event Management*
[2] *Endpoint Detection and Response*

4. Sécurité de l'information et protection des données

4.1. Protection du patrimoine informationnel

Les sociétés et entités du Groupe SEB sont propriétaires de nombreuses informations réparties sur différents supports (papier, dématérialisé etc.). Globalement, les entreprises sont de plus en plus exposées à des actes de prédation de l'information. Les principales menaces sont notamment, la cybercriminalité et l'espionnage industriel. Le recours croissant à la sous-traitance, l'usage accru des technologies de l'information et de la communication telles que le Cloud, les solutions SaaS, le télétravail, la mobilité, la frontière souvent mince entre vie professionnelle et vie privée, et le recours à l'intelligence artificielle contribuent à l'augmentation de ces menaces. Dans ce contexte, le Groupe SEB met en œuvre des solutions techniques et organisationnelles afin de garantir la sécurité de l'ensemble du patrimoine informationnel.

Un effort particulier pourra être mis en œuvre afin de protéger des informations avec un niveau de confidentialité plus élevé ou qui relèvent de cadres juridiques particuliers, y compris les données à caractère personnel décrites ci-dessous.

4.2. Gestion des risques liés aux tiers

Le Groupe accorde une attention particulière à la gestion des risques liés aux tiers. Les fournisseurs, prestataires et partenaires ayant accès aux systèmes d'information ou aux données du Groupe font l'objet de mesures spécifiques incluant des clauses contractuelles de sécurité et de confidentialité, une évaluation proportionnée aux risques (*due diligence*), des exigences d'escalade et de notification en cas d'incident, ainsi qu'une revue périodique des accès.

Ces dispositions s'appliquent notamment aux prestations de cloud, de SaaS, d'infogérance et aux projets impliquant des objets connectés.

4.3. Protection des données personnelles

La politique du Groupe SEB en matière de protection des données personnelles repose sur un socle commun applicable à l'ensemble des marchés dans lesquels le Groupe opère et à toutes les personnes dont les données personnelles sont traitées (notamment les consommateurs, clients, collaborateurs et partenaires). Ce socle de standards Groupe est basé sur le Règlement Général sur la Protection des Données (RGPD) et intègre les réglementations locales lorsqu'elles sont divergentes ou lorsqu'elles complètent le cadre européen. Ce socle repose sur les politiques du Groupe qui définissent les règles de gouvernance et de conformité en matière de protection des données personnelles.

La protection des données personnelles est un enjeu majeur pour le Groupe SEB. Elle constitue un pilier essentiel de son engagement en matière de conformité et de confiance envers ses consommateurs, clients, collaborateurs et partenaires. La protection et le respect de la confidentialité des données personnelles sont d'ailleurs mis en avant comme un des thèmes clés du Code éthique du Groupe. Les pratiques du Groupe s'appuient sur les principes clés de la réglementation sur les données personnelles, déclinés dans ses politiques et standards internes.

Les personnes dont les données personnelles sont traitées par le Groupe disposent de droits (notamment un droit d'accès, de suppression ou de modification), conformément au cadre défini par la législation applicable. Elles doivent également pouvoir compter sur une gestion sécurisée et confidentielle de leurs données personnelles.

Afin de garantir le respect de ces principes, le Groupe :

- met en place des mesures techniques et organisationnelles qui limitent notamment l'accès à ces données aux seules personnes qui ont besoin d'en connaître, aussi bien en interne que pour des tiers extérieurs au Groupe,
- intègre par ailleurs à tout contrat signé avec un fournisseur ou un prestataire tiers des prérequis de sécurité, et de confidentialité, qui sont d'une exigence au moins égale aux standards du Groupe en matière de protection des données personnelles,
- met en œuvre un mécanisme d'alerte qui associe les équipes *data privacy* et cybersécurité, dès la suspicion d'incident afin de réaliser une analyse. En cas d'incident avéré, une *task force* est mise en place pour traiter l'incident et définir un plan de remédiation et une analyse d'impact pour s'inscrire dans un process d'amélioration continue,
- veille à intégrer les principes de *privacy by design* et *privacy by default* dans le développement de ses projets, produits et services impliquant des données personnelles.

4.4. Une organisation en réseau

La gouvernance de la protection des données personnelles au sein du Groupe repose sur le Responsable de la Protection des Données Personnelles (DPO), agissant en toute indépendance et une fonction conformité spécialisée en protection des données personnelles, au sein du département Conformité Groupe. Ces fonctions centrales s'appuient sur un réseau international composé de DPO et *Privacy Relays* afin de :

- garantir le respect de l'application homogène des règles et processus Groupe en matière de protection des données personnelles ;
- accompagner les entités dans la mise en œuvre des exigences réglementaires applicables ;
- renforcer la culture de protection des données personnelles au sein des métiers.

5. Pilotage, indicateurs et amélioration continue

Le Groupe s'appuie sur plusieurs indicateurs de pilotage afin de mesurer l'efficacité de ses dispositifs de sensibilisation et de protection, notamment la fréquence des exercices de gestion de crise, la couverture des campagnes de sensibilisation, la fréquence des tests de phishing, la part des collaborateurs formés aux enjeux de cybersécurité, ainsi que l'existence de processus de revue des incidents et de plans de remédiation.

Le Groupe SEB s'inscrit dans une démarche d'amélioration continue de ses dispositifs de cybersécurité, de sécurité de l'information et de protection des données personnelles. Cette démarche vise à adapter en permanence le niveau de maîtrise des risques aux évolutions du contexte technologique, réglementaire et des menaces.