Votre assistant d'enseignement virtuel, disponible 24/7
pour répondre à vos questions et vous permettre d'apprendre plus efficacement !
Stellia, École Polytechnique, Paris, FRANCE

Stellia

Conformité et procédures RGPD

Version: Janvier, 2023

Votre assistant d'enseignement virtuel, disponible 24/7
pour répondre à vos questions et vous permettre d'apprendre plus efficacement !
Stellia, École Polytechnique, Paris, FRANCE

0.1. Objectif de ce document

Ce document est une déclaration de conformité de la solution Stellia au règlement général sur la protection des données (RGPD) de l'Union européenne. Il présente les données collectées et traitées, la finalité de la collecte, son hébergement et sa sécurité.

Ce document présente également les procédures permettant aux utilisateurs de la solution d'accéder, de corriger ou de supprimer les données qui les concernent, ainsi que la procédure d'information.

Le délégué à la protection des données est la société Dipeeo et peut être contacté à DPO@stellia.ai

Votre assistant d'enseignement virtuel, disponible 24/7
pour répondre à vos questions et vous permettre d'apprendre plus efficacement !
Stellia, École Polytechnique, Paris, FRANCE

---

1. Le règlement RGPD

1.1. Les principes fondateurs du règlement RGPD

Le Règlement Général sur la Protection des Données (RGPD) de l'Union européenne est essentiellement régi par les 8 principes suivants (cf. articles 5.1 et 5.2 du RGPD) sur la collecte, la gestion et le traitement des données personnelles:

1. **Licéité, équité et transparence**: “traitées légalement, équitablement et de manière transparente en relation aux particuliers (“légalité, équité et transparence”);”
2. **Limitation des finalités:** “collectées à des fins déterminées, explicites et légitimes et non traitées ultérieurement d'une manière incompatible avec ces finalités ; le traitement ultérieur à des fins d'archivage dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques ne sera pas considéré comme incompatible avec les finalités initiales (“limitation de la finalité”) “
3. **Minimisation des données**: “adéquate, pertinente et limitée à ce qui est nécessaire par rapport aux finalités pour lesquelles elles sont traitées (“minimisation des données”)”
4. **Exactitude**: “exactes et, si nécessaire, mises à jour ; toutes les mesures raisonnables doivent être prises pour garantir que les données à caractère personnel inexactes, au regard des finalités pour lesquelles elles sont traitées, soient effacées ou rectifiées sans délai (“exactitude”)”
5. **Limitation de stockage**: “conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas la durée nécessaire aux finalités pour lesquelles les données à caractère personnel sont traitées; les données personnelles peuvent être stockées pendant des périodes plus longues dans la mesure où les données personnelles seront traitées uniquement à des fins d'archivage dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques sous réserve de la mise en œuvre des mesures techniques et organisationnelles appropriées requises par le règlement RGPD afin de sauvegarder les droits et libertés des individus (“limitation de stockage”)”
6. **Intégrité et confidentialité (sécurité)**: “traitées de manière à garantir une sécurité appropriée des données à caractère personnel, y compris la protection contre le traitement non autorisé ou illégal et contre la perte, la destruction ou les dommages accidentels, en utilisant des mesures techniques ou organisationnelles appropriées (“intégrité et confidentialité”)”
7. **Responsabilité**: “Le responsable du traitement est responsable du respect du paragraphe 1 (“responsabilité”) et doit être en mesure de le démontrer”

1.2. Les droits de l'utilisateur final du règlement RGPD

Pour permettre aux utilisateurs finaux de contrôler les données liées à leur profil ou à leur activité, le Règlement Général sur la Protection des Données (RGPD) de l'Union européenne demande au responsable du traitement des données de leur offrir les droits suivants :

1. **Accès**: savoir si les données les concernant sont en cours de traitement et y accéder (article 15)
2. **Rectification:** lorsque les données personnelles sont inexactes, les responsables du traitement doivent les corriger (article 16)
3. **Effacement:** demander l'effacement des données ou droit à l'oubli si les données personnelles ont été rendu publiques (article 17)
4. **Limitation du traitement:** demander que le traitement de ses données personnelles soit limité lorsque ce traitement n'est pas essentiel au service fourni à l'utilisateur final (article 18)
5. **Information**: le responsable du traitement doit informer les destinataires qui ont obtenu ces données, dans la mesure du possible. La personne concernée a également le droit de demander «quels sont tous les destinataires ayant pu accéder à mes données» (article 19)
6. **Portabilité des données**: droit d'obtenir les données personnelles qui les concernent dans un format structuré, couramment utilisé et lisible par machine afin de pouvoir les transférer à un autre responsable du traitement (article 20)
7. Le droit d'**opposition:** droit de refus de tout traitement des données personnelles à effectuer ou en cours (article 21)
8. **Droits liés à la prise de décision automatisée et au profilage** : le droit de la personne concernée de ne pas être soumise à une décision fondée uniquement sur un traitement automatisé, y compris le profilage, dans le cas où cette décision produit des effets juridiques la concernant ou l'affecte de manière significative (Article 22)

2. Stellia Déclaration de conformité avec le RGPD

Stellia, société développant et commercialisant la solution Stellia, confirme par le présent document avoir travaillé pour assurer et vérifier la conformité de Stellia avec le règlement RGPD de l'UE et en particulier, ses principes fondateurs et droits des utilisateurs finaux mentionnés ci-dessus.
Stellia s'engage à continuer à travailler pour améliorer ou corriger la conformité de Stellia avec le règlement RGPD, à la suite de toute évolution du produit, mise à jour de la loi ou de recommandations supplémentaires de toute autorité légale ou d'un audit RGPD / données personnelles.

La manière dont Stellia se conforme au règlement RGPD est détaillée dans les chapitres suivants.

3. Détails de la conformité RGPD de Stellia

3.1. Objectif de Stellia et relation avec les données

Stellia est un assistant virtuel d'apprentissage / d'accès à la connaissance.
Stellia vient en complément d'un service d'apprentissage existant fourni à l'utilisateur final par un fournisseur de services, généralement un établissement d'enseignement, un organisme de formation ou une entreprise. Par conséquent :

1. La relation avec l'utilisateur final est la propriété exclusive du fournisseur de services, qui doit couvrir les impacts de Stellia sur la collecte et le traitement des données personnelles dans son information aux utilisateurs finaux (voir 3.5. Mise à jour des Conditions Générales d'Utilisation du client)
2. Pour identifier l'utilisateur final d'une session à une autre, notamment pour lui montrer son historique de questions & réponses, ou suivre sa progression dans les apprentissages, Stellia s'appuie sur :
    - soit son propre identifiant utilisateur unique, généré automatiquement lors de la première session de l'utilisateur et stocké dans une session utilisateur à l'aide d'un cookie. Cet identifiant est généré de manière aléatoire et n'est pas associé à des informations personnellement identifiables (PII).
    - ou un identifiant unique de l'utilisateur fourni par le fournisseur de services via sa plateforme d'apprentissage (LMS). Cet identifiant de l'utilisateur peut être anonymisé à l'aide d'une fonction de hachage qui ajoute une couche de pseudonymisation empêchant

quiconque d'identifier l'utilisateur final, même en accédant aux données de Stellia et du fournisseur de services en même temps, sans connaître la fonction de hachage et sa clé.

- pour le service d'ancrage des connaissances, l'apprenant doit accepter des Conditions Générales d'Utilisation et fournir une adresse email afin de recevoir régulièrement (jusqu'à une fois par jour) des sollicitations pour vérifier la persistance en mémoire des connaissances / compétences récemment acquises

3. Pour améliorer et personnaliser son service aux utilisateurs finaux, Stellia collecte et stocke les événements d'interaction les plus importants de l'utilisateur final avec son service d'assistant virtuel, et peut collecter d'autres événements d'interaction sur le service principal (principalement des activités d'apprentissage) par le prestataire de services grâce à une API.

3.2. Minimisation des données, collecte des données et finalité

Stellia s'engage à respecter le principe de **minimisation des données**, c'est-à-dire à limiter la collecte de données à son minimum pour assurer le service. Cependant, pour offrir la meilleure expérience de support d'apprentissage à ses utilisateurs finaux, Stellia est également disposé à personnaliser ses services à chaque utilisateur et au contexte, ainsi qu'à améliorer continuellement son service et doit ainsi collecter une importante variété de données concernant l'utilisateur final, son activité et son interaction avec le service et ses fonctionnalités.
Plus précisément, Stellia s'appuie sur plusieurs modèles d'intelligence artificielle dont les performances augmentent considérablement avec la quantité de données collectées ; de nombreuses fonctionnalités et événements peuvent fournir des entrées précieuses pour optimiser les sorties de notre modèle d'IA et ainsi améliorer les performances du service fourni à l'utilisateur final.

Stellia peut collecter et stocker les données suivantes :

Nom des données	Détails des données collectées	Objectifs de la collecte de données
Identifiant pseudonymisé unique de l'utilisateur final	● pseudonyme de l'utilisateur (le format dépend de l'identifiant du fournisseur de services)	● Pour fournir le service spécifiquement à l'utilisateur concerné ● Pour stocker et afficher l'historique de l'utilisateur dans différentes sessions ● Pour créer un profil utilisateur et adapter le service à l'utilisateur ● Pour pouvoir traiter les demandes relatives au règlement RGPD des utilisateurs finaux ● Pour constituer des statistiques d'usage du service, comme le volume d'utilisateurs uniques par jour

stellia

Votre assistant d'enseignement virtuel, disponible 24/7
pour répondre à vos questions et vous permettre d'apprendre plus efficacement !

Stellia, École Polytechnique, Paris, FRANCE

Uniquement si activation du service d'ancrage des connaissances		
Email de l'utilisateur	• Adresse email de l'utilisateur	• Pour adresser à l'utilisateur des emails réguliers testant et renforçant l'ancrage en mémoire des connaissances précédemment acquises. Une sollicitation "push" par email permet un engagement plus fort et régulier de l'utilisateur qu'une interface accessible librement par l'apprenant Le consentement de l'utilisateur (CGU, mentions légales et informations données personnelles RGPD) est recueilli à la collecte.
Pour tous les services		
Événements suggestions de questions	• question utilisateur (texte) • questions suggérées et score d'association (ids, valeurs) • question sélectionnée par l'utilisateur (id) • contexte / page (id)	• Pour suggérer les questions les plus pertinentes pour chaque utilisateur en fonction de sa question en cours de saisie • Pour ajuster la force des liens entre les questions et les concepts de connaissances et optimiser l'arbre de connaissances de Stellia utilisé par les services d'apprentissage adaptatif et de rétention des connaissances
Événements questions / réponses	• question utilisateur (texte) • question / réponse associée dans la base de données Stellia (id) • score d'association (valeur décimale) • contexte / page (id)	• Pour fournir une réponse pertinente à une question de l'utilisateur final • Pour personnaliser les réponses aux questions des utilisateurs en fonction de l'historique des conversations de l'utilisateur avec Stellia • Pour analyser les questions des utilisateurs et mieux comprendre leurs besoins par rapport à la base de données de connaissances de Stellia • Pour surveiller les centres d'intérêts et les difficultés des utilisateurs finaux et mieux personnaliser le service d'apprentissage adaptatif
Événements sélection de questions liées	• question utilisateur (texte) • questions associées proposées & score d'association (ids, valeurs) • question associée sélectionnée par	• Pour en savoir plus et proposer les questions connexes les plus pertinentes pour chaque utilisateur en fonction de son historique de questions et de la sélection de questions connexes • Pour ajuster la force des liens entre les questions et les concepts de connaissances et optimiser l'arbre de connaissances de Stellia utilisé par les services d'apprentissage adaptatif et de rétention des

	l'utilisateur (id) • contexte / page (id)	connaissances
Événements Réponses Experts	• question utilisateur (texte) • question / réponse la plus pertinente dans la base de données Stellia (id) • score d'association (valeur) • réponse d'expert (texte) • contexte / page (id)	• Pour analyser la similarité d'une réponse d'expert / enseignant avec les réponses de Stellia pour la question associée
Événements de notation des réponses	• question / réponse dans la base de données Stellia (id) • niveau de notation (flottant)	• Pour comprendre les préférences de réponse de l'utilisateur et sélectionner la réponse la plus pertinente pour chaque utilisateur et sa question • Pour identifier, analyser et remplacer les réponses impopulaires
Événements d'apprentissage	• Type d'interaction de l'utilisateur avec le contenu (texte) • contenu d'apprentissage (id) • score (flottant, optionnel) • contexte / page (id)	• Pour mesurer la maîtrise par l'utilisateur de chaque concept de connaissance et donc : • Pour évaluer et renforcer la rétention des connaissances précédemment acquises par chaque utilisateur (service d'ancrage des connaissances) • Pour personnaliser le parcours d'apprentissage pour chaque utilisateur (service d'apprentissage adaptatif)
Données supplémentaires pour tous les événements	• timestamp • user agent • user id (id) • contexte / page (id)	• Les informations de l'User Agent permettent d'optimiser l'expérience utilisateur (notamment la taille de l'écran et les capacités de son terminal) et offrir des fonctionnalités spécifiques au client. Il permet également de prioriser le développement des services Stellia pour des terminaux spécifiques en fonction du volume d'utilisateurs finaux associé. • Le contexte est essentiel pour adapter la réponse aux questions, la rétention des connaissances et les services d'apprentissage adaptatif

Stellia ne stocke pas les informations personnellement identifiables (PII) telles que:

- nom d'utilisateur, prénom, numéro de téléphone, mot de passe *
- adresse e-mail, hormis si le service d'ancrage des connaissances est activé
- adresse IP de l'utilisateur** , coordonnées GPS, emplacement précis ou adresse physique
- Données financières ou de santé de l'utilisateur

* L'utilisateur final est authentifié par le fournisseur de services intégrant Stellia ou n'est pas authentifié (lors de l'utilisation de l'extension Stellia)
** L'adresse IP de l'utilisateur est obtenue mais uniquement quelques chiffres sont stockés

3.3. Stockage des données

Pour les services en Europe, les données utilisateur collectées par Stellia sont stockées sur un stockage cloud situé en France, ou dans l'Union européenne, et fourni par Amazon Web Services (AWS).
Le stockage des données est limité à une période de 18 mois, comme recommandé par l'Union européenne. Les données sont régulièrement sauvegardées et les données datant de plus de 18 mois sont régulièrement effacées.

3.4. Sécurité des données

Stellia consacre des efforts importants pour appliquer les principes de sécurité à l'état de l'art, tels que:

- disposer d'experts en sécurité pour concevoir une architecture sécurisée et appliquer les principes de sécurité standard de solutions SaaS
- assurer une veille technologique pour sélectionner les outils les plus sécurisés, et pallier aux failles de sécurité publiées relatives aux composants logiciels utilisés,
- mettre en oeuvre des mises à jour logicielles régulières pour corriger les problèmes de sécurité,
- sensibiliser et former l'équipe de Stellia à la sécurité.

En ce qui concerne les données utilisateurs et leur hébergement, en tant que leader mondial de l'hébergement cloud, AWS propose une large gamme de services de sécurité pour protéger les services et données clients.

Du côté de Stellia, les données des utilisateurs ne peuvent être accédées ou modifiées que par:

1. l'interface Stellia lorsqu'utilisée par les utilisateurs finaux (accédant et mettant à jour uniquement quelques-unes de leurs propres données utilisateur)
2. le service de statistiques de Stellia pour collecter et stocker l'activité des utilisateurs (uniquement accès aux données)

3. et les administrateurs de la base de données, en particulier pour fournir des analyses spécifiques demandées par le fournisseur de services.

Tous interagissent avec les données via nos API et sont authentifiés via des services d'authentification sécurisés, empêchant tout accès et modification des bases de données utilisateurs non légitimes.
De plus, tous les accès en lecture et en écriture aux données de l'utilisateur sont enregistrés, ce qui permet une enquête en cas d'accès inconnu ou indésirable.

3.5. Mise à jour des Conditions Générales d'Utilisation du fournisseur de services

Pour garantir que chaque utilisateur donne son consentement éclairé après avoir été informé de manière complète et claire de la collecte et du traitement des données générées par ses activités, ainsi que de ses droits sur ces données, **le fournisseur de services de l'utilisateur final**, fournissant le service aux utilisateurs finaux, **doit s'assurer que ses Conditions Générales d'Utilisation contiennent les éléments suivants**:

1. Les données mentionnées ci-dessus sont répertoriées comme des données collectées avec leur finalité de traitement.

2. Stellia, fournisseur de Stellia, assistant virtuel d'enseignement, est cité comme sous-traitant pour le traitement des données.

3. Les Conditions Générales d'Utilisation (CGU) expliquent le processus permettant aux utilisateurs finaux d'accéder, de mettre à jour ou de supprimer les données attachées à leur profil.
   Dans un tel cas, le fournisseur de services utilisant le service Stellia doit contacter le Délégué à la Protection des Données ou Data Protection Officer de Stellia (dpo@stellia.ai) pour traiter la demande de l'utilisateur final, voir le chapitre suivant Procédures

4. Procédures RGPD

A ce jour, les données relatives à un utilisateur sont associées à un id pseudonymisé et ne peuvent donc être associées à un utilisateur identifiable. En conséquence, dans ce cas, les données n'ont pas de caractère personnel et les droits prévus par le règlement RGPD ne sont pas strictement applicables mais Stellia prévoit tout de même leur mise en œuvre.

D'un point de vue pratique, par construction, Stellia est incapable d'identifier les données à un utilisateur final qui nous contacterait par email afin d'accéder à ses données personnelles ; le fournisseur de services devra donc générer et fournir à Stellia l'id pseudonymisé utilisé pour l'utilisateur final.

La seule exception concernant le caractère personnel des données est le service d'ancrage des connaissances pour lequel l'adresse email est collectée et les données collectées sont donc associées à un utilisateur identifiable. Dans ce cas, les procédures RGPD décrites ci-dessous sont opérationnelles sans avoir besoin de générer l'id pseudonymisé.

4.1. Procédure générale de traitement des demandes RGPD des utilisateurs

1. Comme Stellia n'est pas propriétaire de la relation client avec l'utilisateur final, toutes les demandes de l'utilisateur final doivent être directement adressées au fournisseur de services, par exemple grâce à un formulaire en ligne dédié ou via une adresse e-mail dédiée.

2. Avant de répondre à une demande d'un utilisateur final, le fournisseur de services doit:

    a. vérifier la validité de la demande, conformément au règlement RGPD, voir 1.2. Les droits de l'utilisateur final du RGPD. En règle générale, un utilisateur final peut demander à ce que ses données utilisateur soient corrigées, mais si la modification demandée est manifestement invalide (ex: âge = 150, nom = Ano Nymous…), suspecte ou malveillante, le fournisseur de services doit collecter des preuves de la validité de la demande, avant d'accepter de la traiter.

    b. vérifier l'identité de l'utilisateur tel qu'inscrit sur son service, par exemple en envoyant un e-mail à l'utilisateur final concerné pour lui demander sa confirmation explicite qu'il est bien à l'origine de la demande. En règle générale, une adresse e-mail d'origine peut facilement être falsifiée, donc recevoir une demande de suppression d'un compte de l'e-mail d'un utilisateur ne signifie pas nécessairement qu'elle a été créée par ce même utilisateur. Accéder à un email adressé à un utilisateur est par contre admis comme une preuve de l'identité du demandeur (il est malheureusement quasiment impossible de se prémunir d'un cas plus complexe, heureusement rare, où un hacker est en capacité d'accéder et d'utiliser son adresse email).

L'équipe de Stellia, ne possédant pas la relation avec l'utilisateur final et ne possédant donc aucune de ses coordonnées de contact, n'est pas en mesure de joindre directement l'utilisateur final pour effectuer un contrôle, considérera que ces deux contrôles ont été traités par le prestataire de services et donc n'exécute aucun contrôle de son côté, sauf dans le cas où la demande est manifestement invalide ou hautement suspecte.

3. Une fois la validité de la demande et l'identité du demandeur vérifiées, le fournisseur de services traitera la demande. Le fournisseur de services enverra ensuite une demande à dpo@Stellia avec:
    a. la demande de l'utilisateur final
    b. si le service d'ancrage des connaissances n'est pas actif, l'identifiant unique de l'utilisateur final (pseudonyme) utilisé avec le service Stellia **sans toute information personnellement identifiable (PII),** telle que nom, prénom, adresse physique ou e-mail. Par conséquent, le service fourni doit les supprimer avant de communiquer la demande à Stellia.
    c. si le service d'ancrage des connaissances est actif, l'adresse email de l'utilisateur final utilisé avec le service Stellia

4. Considérant que la validité de la demande et l'identité du demandeur ont été dûment vérifiées par le fournisseur de services, les administrateurs de la base de données Stellia traiteront la demande de l'utilisateur final, et confirment son traitement ou délivrent son résultat au fournisseur de services, afin qu'il puisse fournir la confirmation ou la réponse à l'utilisateur final.

4.2. Délai de traitement des demandes RGPD des utilisateurs finaux

Il convient de noter que le délai recommandé pour traiter une demande d'utilisateur final est de 72H. Comme Stellia ne peut garantir un délai de traitement inférieur à 2 jours ouvrés, le fournisseur de services fournira au plus vite à l'équipe de Stellia les informations nécessaires pour traiter la demande de l'utilisateur final.
Le délai de traitement est dû au temps nécessaire pour libérer une ressource interne accréditée pour répondre à la demande, et non au délai du processus technique.

4.3. Traitement des demandes RGPD des utilisateurs finaux

S'appuyant sur des bases de données SQL pour le stockage des données relatives aux utilisateurs finaux, l'administrateur de la base de données Stellia peut facilement traiter les principales demandes relatives au règlement RGPD des utilisateurs finaux :

- Demande d'accès → Requête SQL GET sur l'ID utilisateur
- Requête de rectification → Requête SQL UPDATE sur l'ID utilisateur
- Demande d'effacement / Droit à l'oubli → Requête SQL DELETE sur l'ID utilisateur

Pour la **restriction de traitement ou le droit d'opposition**, à la demande de l'utilisateur final, Stellia est en mesure d'arrêter la collecte d'événements utilisateur d'un utilisateur et ne s'appuyer que sur le contexte pour prendre en charge l'utilisateur final ; ceci implique de désactiver toute personnalisation du service Questions / Réponses. Cependant, cela désactive également les services d'ancrage des connaissances et d'apprentissage adaptatif qui reposent fortement sur les données des utilisateurs et la personnalisation.

En ce qui concerne l'information des utilisateurs à propos des destinataires des données utilisateurs, Stellia ne partage actuellement les données avec aucune tierce partie. Dans le cas où Stellia serait amené à partager des données utilisateurs avec une tierce partie, le fournisseur de services sera informé avec un délai préalable raisonnable afin qu'il puisse informer les utilisateurs finaux à ce sujet avant la mise en œuvre d'un tel partage.

Pour la portabilité des données, à la demande de l'utilisateur, Stellia peut fournir toutes les données utilisateur au format JSON, avec des des champs explicites, afin de permettre leur exploitation par tout autre fournisseur de services.

Les droits relatifs à la prise de décision automatisée et au profilage ne s'appliquent pas aux traitements de Stellia, car le traitement des données de Stellia est uniquement destiné à aider l'utilisateur final et n'est pas censé avoir un effet juridique ou financier ou de santé sur l'utilisateur.

4.4. Informations des utilisateurs suite à une faille de sécurité

Quels que soient les efforts déployés pour maximiser la sécurité des données, aucune organisation ne peut prétendre être à l'abri de failles de sécurité et d'accès non autorisé à ses données. Il existe de nombreux exemples de failles de sécurité exploitées auprès d'organisations très sensibles quant à la sécurité (services publics, services de renseignement, finance…) et certains hackers sont parrainés par des États et ont accès à des vulnérabilités zero-day, inconnues de la plupart des experts en sécurité.

Ainsi, au-delà de l'effort de Stellia consacré à mettre en œuvre en permanence les normes de sécurité les plus élevées relatives à son activité, une procédure spécifique a été conçue pour organiser la détection, la gestion et la communication en cas d'exploitation d'une faille de sécurité indésirable.

4.4.1. Détection d'une faille de sécurité

Comme tous les accès et opérations sur les données des utilisateurs sont journalisés:

1. Stellia vérifie régulièrement le volume de ces opérations par type d'opérations et les ratios entre les volumes de ces types d'opérations pour identifier les volumes ou ratios anormaux et rechercher si ceux-ci peuvent être expliqués par les opérations de service ou sont suspects.
   Il est prévu de continuellement renforcer les alertes automatiques dans les prochains mois, sur la base de l'expérience acquise par Stellia sur les niveaux normaux et anormaux pour s'assurer que seules les alertes pertinentes sont déclenchées.

2. En outre, Stellia analyse régulièrement des échantillons de journaux pour vérifier la cohérence ou repérer toute anomalie.

De plus, en exécutant une veille technologique et de sécurité, Stellia est rapidement informé de la découverte de nouvelles vulnérabilités sur les outils utilisés, si de telles vulnérabilités ont déjà été exploitées et des moyens de détecter de telles failles de sécurité. Évidemment, Stellia s'engage à mettre à jour les outils qu'il utilise dans les plus brefs délais, notamment en cas de découverte de vulnérabilité et de disponibilité d'un correctif.

4.4.2. Gestion d'une faille de sécurité: enquête, confinement, correction

En cas de découverte d'une faille de sécurité affectant les systèmes de Stellia, la réaction doit être traitée de manière ordonnée:

1. Pour arrêter la faille de sécurité, idéalement, le maximum d'information à propos de la faille de sécurité doit être rapidement collecté pour mieux comprendre la vulnérabilité, son périmètre

exact et ses impacts, et identifier les moyens de résolution.
Pour améliorer l'analyse, des journaux plus détaillés peuvent être rapidement activés et des outils de surveillance supplémentaires peuvent être déployés.

2. Ensuite, le plus rapidement possible, souvent avant d'avoir une compréhension complète de la faille, des efforts importants doivent être déployés pour arrêter la faille de sécurité, parfois d'abord par des moyens temporaires ou des solutions d'urgence lorsque la solution définitive n'est pas encore parfaitement définie ou a besoin de beaucoup de temps pour être déployée.
   Parfois aussi, la solution la plus rapide à déployer ne limite que partiellement la faille de sécurité et ses impacts.
   Cependant, malgré l'urgence, une attention particulière sera consacrée à l'analyse des différentes solutions possibles pour éviter d'introduire des vulnérabilités supplémentaires.
   Différentes solutions peuvent être étudiées en fonction de la faille de sécurité et de son analyse, comme, entre autres, le déploiement urgent d'un correctif de sécurité disponible, la réinitialisation de toutes les informations d'identification pour l'accès au système ou le blocage de toutes les connexions entrantes au-delà d'un réseau de confiance.
   Dans le pire des cas, cela peut conduire à la désactivation de certaines fonctionnalités ou même à l'indisponibilité temporaire du service pour l'utilisateur final.

3. Lorsque la faille de sécurité a été bloquée par des moyens temporaires, ou du moins considérablement limitée, l'équipe dispose de plus de temps pour concevoir, construire et déployer une solution définitive.

4. Dans le cadre de la première étape, l'enquête doit être poursuivie:
   a. pour mieux comprendre si la faille de sécurité a été entièrement corrigée
   b. pour mieux comprendre les impacts et l'étendue de la faille de sécurité: quelles données et quels systèmes ont été accédés, en particulier comprendre si la faille a mené "seulement" à un accès ou à une modification / altération des données
   c. pour tenter de recueillir des informations sur l'auteur de la faille de sécurité (lorsque l'attaque est sophistiquée, cette tentative peut être vaine, mais parfois, les résultats peuvent être rapides)

5. Enfin, au cas où des données ont été modifiées, Stellia peut déployer des sauvegardes de données car l'hébergement AWS sauvegarde régulièrement les données.

6. En conclusion, des tests de sécurité internes et un audit de sécurité externe peuvent être menés afin qu'une telle faille de sécurité ne puisse plus se produire et vérifier que sa correction n'a pas introduit de vulnérabilité supplémentaire.

7. Une analyse “post-mortem”, idéalement réalisée avec l’accompagnement d’un cabinet expert en sécurité informatique, sera menée afin d’éviter toute reproduction d’une telle faille et améliorer les procédures de sécurité.

4.4.3. Communication en cas de faille de sécurité

Le règlement RGPD oblige les organisations qui collectent les données des utilisateurs à communiquer de toute urgence aux utilisateurs finaux toute faille de sécurité et son impact sur les données des utilisateurs.

Comme Stellia n'est pas propriétaire de la relation utilisateur final, Stellia ne communique qu'avec le fournisseur de services propriétaire de la relation utilisateur final et s’appuie sur le fournisseur de services pour assurer la communication avec les utilisateurs finaux.

Dans le cas où Stellia détecte une faille de sécurité, il communiquera toutes les informations disponibles au fournisseur de services dans un délai maximum de 4 heures après la découverte de la faille de sécurité, idéalement avec les détails suivants :

- Informations sur l'événement de violation de sécurité :
  - Période de la faille de sécurité
  - Utilisateurs impactés ou potentiellement impactés
  - Données exposées
  - Impacts sur les données de l'utilisateur (accès ou modification) et les utilisateurs (impacts sur le fonctionnement du service, impacts utilisation des données exposées en dehors du service, en l’occurrence l’accès à l’adresse email permet aux hackers d’inclure l’utilisateur dans des bases de destinataires de spam / emails de phishing et de tenter l’accès à d’autres services via l’adresse email récupérée et des mots de passe faibles)
- Toute mesure de correction ou de prévention à appliquer par l'utilisateur final
- Toute mesure de correction ou de prévention à appliquer par le fournisseur de services
- Les efforts menés par Stellia pour corriger, atténuer et enquêter sur la faille de sécurité

Une communication quotidienne sera menée par Stellia avec le fournisseur de services pour lui partager toutes les nouvelles informations jusqu'à ce qu'une correction définitive ait été déployée et que toutes les informations sur la faille de sécurité aient été collectées et les analyses aient pu conclure.