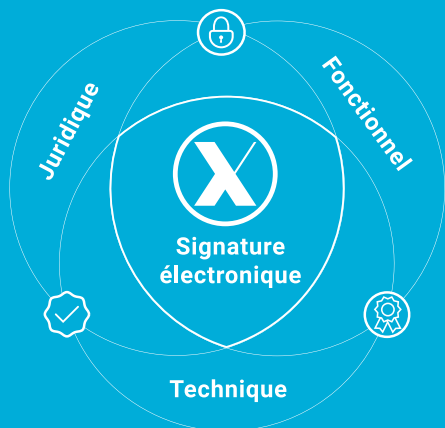
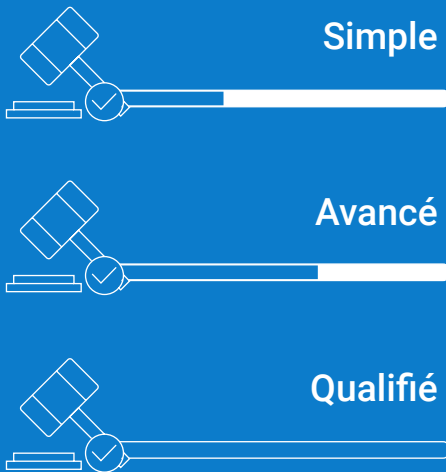
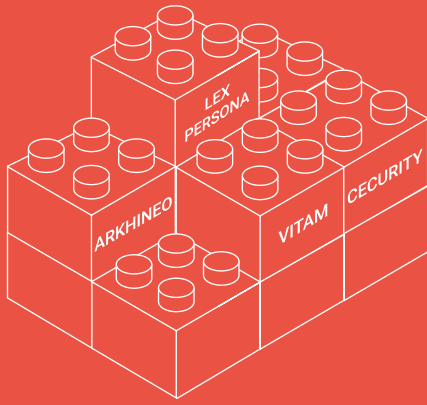
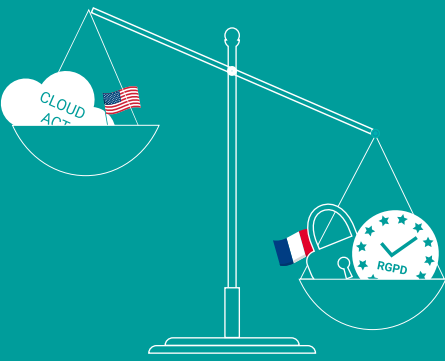


LIVRE BLANC

La signature électronique et son intégration : les clés pour réussir



Sommaire

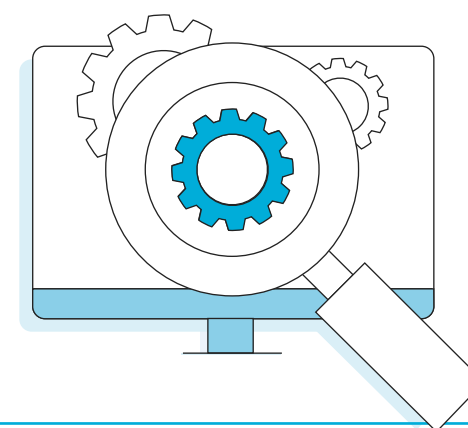
 Introduction	 01	 02	 03	 Retours d'expérience
Les trois facettes de votre projet d'intégration de la signature électronique p.4	Comment adapter le niveau en fonction du risque ? p.8	Comment l'intégrer dans son système d'information ? p.14	Avec quelle garantie en matière de sécurité et de confidentialité ? p.20	Coffreo p.24 Relais Pick-up p.26 Aéroports de Paris p.28
	Le Référentiel Général de Sécurité (RGS) Le règlement eIDAS Les niveaux de sécurité	L'intégration avec FranceConnect Simplifier le parcours utilisateur	Un éditeur de signature électronique qui n'est pas soumis au Cloud Act Points de vigilance autour du RGPD Les certifications, clef de voûte de la conformité et de la pérennité de vos signatures Intégrer une démarche « security by design »	

Introduction

Un projet de signature électronique comprend toujours trois facettes : l'une fonctionnelle, l'autre juridique et la dernière technologique. Chacune de ces facettes doit être finement étudiée pour que le projet soit réussi et adapté au cas d'usage envisagé.

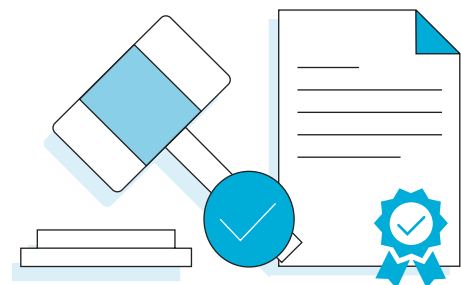
Fonctionnel
Juridique
Technologique

Lorsqu'il s'agit de mettre en place la signature électronique dans une organisation, il faut tout d'abord prendre en compte chaque cas d'usage envisagé en les regardant sous trois angles différents, mais complémentaires :



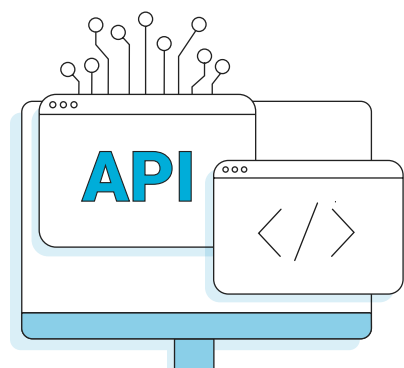
L'angle **fonctionnel** tout d'abord.

L'organisation dématérialise un processus papier existant ou met en place un nouveau processus informatisé et lui greffe la signature électronique. Il est alors fondamental de bien **prendre en compte la manière dont ce processus va fonctionner en relation avec les personnes concernées** : utilisateurs, signataires, destinataires des documents, etc. Bien souvent, un accompagnement au changement est nécessaire. Celui-ci doit prendre en compte les aspects spécifiques aux métiers impactés et le fait que **les habitudes liées au papier n'ont plus de sens**. À titre d'exemple, il n'est plus nécessaire de parapher chaque page d'un document, ou d'en faire une copie pour l'archivage, mais il est en revanche indispensable de les classer, selon une nomenclature adaptée afin de pouvoir les retrouver facilement.



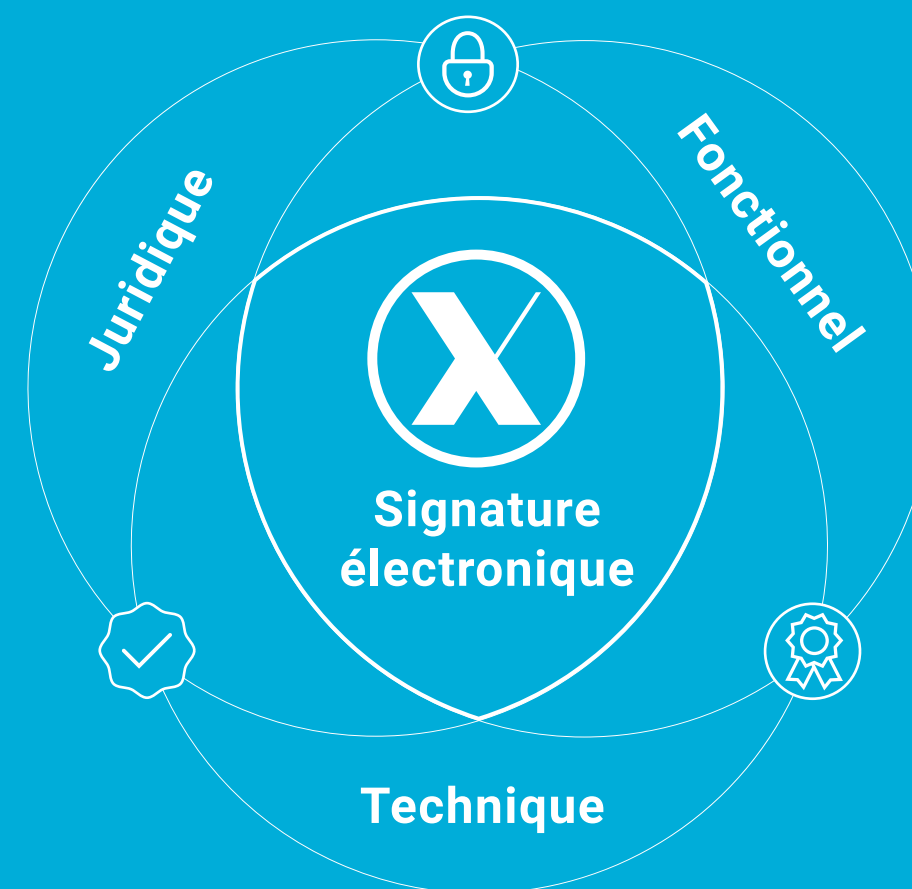
Ensuite, l'angle **juridique**.

Il ne faut pas perdre de vue que la signature d'un document, électronique ou pas, a pour objectif de **créer un acte juridique**. Il est donc essentiel de bien définir le niveau juridique requis par les signatures électroniques mises en œuvre : simple, avancé ou qualifié au sens du règlement eIDAS, RGS 1* ou 2* pour les signatures internes à l'administration, etc. Le cas d'usage envisagé est-il soumis à une réglementation ? Est-il nécessaire d'adapter le niveau de sécurité technique aux risques jurisprudentiels liés à des exigences réglementaires laxistes ou inexistantes ?



Enfin, l'angle **technologique**.

La **signature électronique** se démocratise et se généralise peu à peu dans les organisations. Elle **est amenée à devenir une brique essentielle du système d'information**. C'est ici qu'il est souvent indispensable de faire intervenir la DSI, le RSSI et/ou le DPO. De plus, l'intégration de la signature électronique aux applications métier, à la GED ou au SAE de l'entreprise peut nécessiter des développements faisant intervenir des APIs. Il s'agit de s'assurer de la cohérence des interfaces utilisées afin de faciliter leur maintenabilité et leur évolution.



Un équilibre à trouver

La signature électronique est l'une des rares technologies à englober ces trois aspects. Il est impératif de paramétrer la solution en tenant compte des exigences de ces trois dimensions. Un peu à la manière d'un **tabouret à trois pieds**, c'est un équilibre à trouver. Selon la taille, le fonctionnement et les besoins de votre organisation, les enjeux sont différents. Lex Persona sait justement créer et gérer cet équilibre.

01

Signature électronique : comment adapter le niveau en fonction du risque ?

Ces vingt dernières années, la signature électronique s'est progressivement répandue dans tous les secteurs de l'économie, privés comme publics, avec une relative discrétion, dans un contexte de transformation numérique progressive. Depuis le début de la crise sanitaire, force est de constater une **accélération du mouvement**. Peu à peu, la signature électronique se met au service des collaborateurs d'entreprises, certes, mais aussi des élus, des agents et des citoyens, avec des **besoins de sécurité très diversifiés**.

Si l'usage de la signature électronique est simple et si ses avantages ne sont plus à vanter (praticité, sécurité, traçabilité, gain de temps, etc.), bon nombre d'organisations s'interrogent encore sur la façon de la déployer. **Quels documents** sont concernés ? **Quel** est leur **circuit** ? **Quels** sont les **processus** internes de validation ? **Quel volume** cela représente-t-il ? **Qui** peut signer ? Avec **quel niveau** de signature ? Autant de questions dont les réponses doivent permettre d'établir un cahier des charges en concertation avec la DSI.

À chaque cas d'usage son niveau de signature électronique !

La signature électronique est encadrée par deux dispositifs réglementaires distincts :

Le Référentiel Général de Sécurité (RGS)

→ Le Référentiel Général de Sécurité (RGS) vise à renforcer la sécurité et la confiance dans les échanges au sein de l'administration et avec les citoyens. Il propose trois niveaux de sécurité :

Elémentaire RGS*	Standard RGS**	Renforcé RGS***
Notez que les niveaux « Standard » et « Renforcé » nécessitent une vérification en face à face de l'identité du signataire et l'utilisation d'une clé sécurisée (carte à puce ou clé USB).		

Le règlement européen eIDAS

→ Le règlement européen eIDAS sur l'identification électronique et les services de confiance prévoit, pour sa part, la génération d'une signature (dite) « simple », avancée ou qualifiée. Avec ce règlement, l'Union européenne s'est dotée d'un socle juridique encadrant l'usage de la signature électronique afin de développer son usage. Il définit trois niveaux de signature électronique :

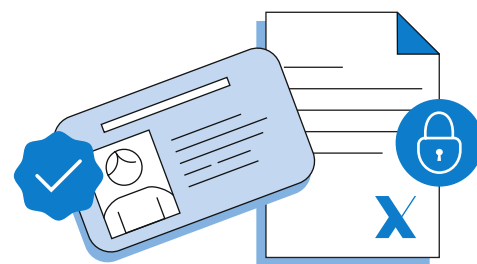
Signature simple	Signature avancée	Signature qualifiée
---------------------	----------------------	------------------------



La signature électronique dite « simple »

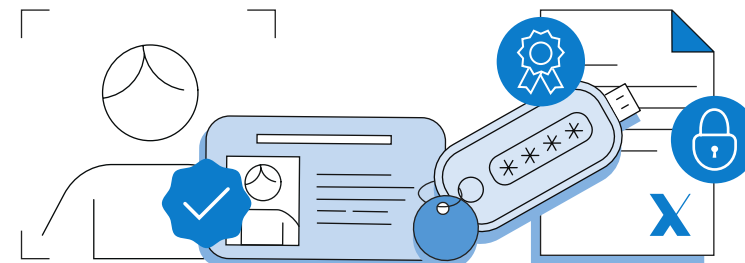
Elle correspond au premier stade de sécurité dans la mesure où elle n'est constituée que de « données sous forme électronique, qui sont jointes ou associées logiquement à d'autres données sous forme électronique et que le signataire utilise pour signer ».

Son objectif est essentiellement de ne discriminer aucune forme de signature électronique, y compris la simple mention d'un nom à la fin d'un courriel. Ce type de signature n'est pas défini dans le droit français.



La signature électronique « avancée »

Elle répond à 4 exigences du règlement eIDAS : elle est **liée sans ambiguïté au signataire** et permet l'**identification** de ce dernier, elle offre un **niveau de confiance élevée** quant à sa mise en œuvre par le signataire et elle garantit l'**intégrité** de l'acte qui en résulte. Ce niveau de signature offre le meilleur compromis en matière de sécurité, de coût, de facilité d'usage et de mise en œuvre.



La signature électronique « qualifiée »

C'est la plus sécurisée des signatures électroniques, et la seule à offrir la même valeur juridique qu'une signature manuscrite dans tous les États membres de l'UE. C'est une signature avancée qui **repose sur un certificat qualifié de signature électronique ainsi que sur un dispositif qualifié de création de signature**. De manière concrète, ce type de signature nécessite une vérification en face à face de l'identité du signataire et l'utilisation d'une clé sécurisée. Elle a vocation à être utilisée principalement pour des raisons de conformité réglementaires. La signature électronique de niveau qualifié eIDAS est préconisée pour les échanges contractuels avec l'étranger. Les signatures de niveau inférieur n'offrent pas la même valeur que la signature manuscrite mais n'en restent pas moins recevables comme preuve en justice.

Notez que des travaux de mise à jour du RGS sont en cours afin de simplifier son articulation avec le règlement eIDAS.

In fine, c'est à chacun d'évaluer le niveau de risque de la transaction ou de jauger de la fiabilité de l'autre partie afin de choisir le niveau de signature électronique adapté à l'opération et ses enjeux. Simple, avancée ou qualifiée ? Pour le code du commerce, une signature électronique « simple » suffit. Mais en cas de réels doutes sur l'autre partie, lors d'un accord avec un fournisseur ou un client peu ou mal connu, il peut être judicieux d'opter pour une signature électronique « avancée » ou « qualifiée ».

	Simple	Avancée	Qualifiée
Caractéristiques principales	Doit désigner le signataire et être rattachée au document	Doit respecter l'article 26 du règlement eIDAS : 1/ être liée au signataire sans ambiguïté 2/ permettre d'identifier le signataire 3/ être créée à l'aide de données que le signataire peut, avec un niveau de confiance élevé, utiliser sous son contrôle exclusif 4/ être liée aux données signées de telle sorte que toute modification ultérieure soit détectable	Doit être une signature avancée et utiliser un certificat qualifié eIDAS associé à un dispositif de création de signature lui aussi qualifié eIDAS
Avantages	/ Facilité de mise en oeuvre / Contraintes d'identification très souples (celle-ci peut être purement déclarative) / Contraintes d'authentification très souples (celle-ci peut être limitée à la simple possession du document à signer)	/ Niveaux de garantie d'identification et d'authentification du signataire proportionnés aux risques juridiques / Rapport équilibré entre le coût et la facilité de mise en oeuvre et d'usage / Garantie de l'intégrité du document signé	/ Niveau de sécurité très élevé / Equivalence avec la signature manuscrite / Renversement de la charge de la preuve / N'impose pas une gestion du contexte et de la traçabilité de la transaction de signature en vue de garantir sa valeur probatoire
Inconvénients	/ L'identification du signataire n'est pas garantie / L'authentification du signataire n'est pas garantie / L'intégrité du document signé n'est pas garantie	/ Nécessite un moyen d'identification permettant d'identifier avec précision le signataire / Nécessite un moyen d'authentification qui peut être contraignant pour l'utilisateur / Nécessite des ressources cryptographiques pour garantir l'intégrité du document et sa relation au signataire.	/ Requiert une vérification en face à face de l'identité du signataire à partir de documents d'identités qui doivent eux-mêmes être vérifiés / Requiert un moyen d'authentification pouvant être complexe à utiliser : support physique, application mobile spécialisée, prérequis techniques sophistiqués... / Coûts de mise à disposition et d'exploitation plus élevés
Usages	Adaptée aux actes juridiques qui présentent un niveau de risque faible ou plus élevé lorsqu'elle est complétée par des moyens de preuve complémentaires et proportionnés au risque ainsi qu'aux niveaux d'identification / d'authentification du signataire et de conservation du document Exemples : commande d'un bien de faible valeur, demande de congés, contrat de travail, etc.	Adaptée aux actes juridiques qui présentent un niveau de risque moyen ou plus élevé lorsqu'elle est complétée par des moyens de preuve complémentaires et proportionnés au risque ainsi qu'aux niveaux d'identification / et d'authentification du signataire et de conservation du document. Exemples : commande d'un bien de valeur élevée, bail commercial, etc.	Adaptée aux actes juridiques qui présentent un niveau de risque élevé Exemples : contrat d'assurance-vie, diplôme, acte d'engagement d'un appel d'offres, etc.



Moins de papier et plus de temps au service des clients

Le choix et le déploiement d'une solution de signature électronique peuvent tirer parti d'un accompagnement adapté aux besoins fonctionnels et réglementaires des organisations.

Mais sa mise en place offre un ROI (« retour sur investissement ») rapide avec à la clé des bénéfices très significatifs : une économie sur les coûts papier et une réduction des délais de signature pour les clients, fournisseurs ou les collaborateurs.

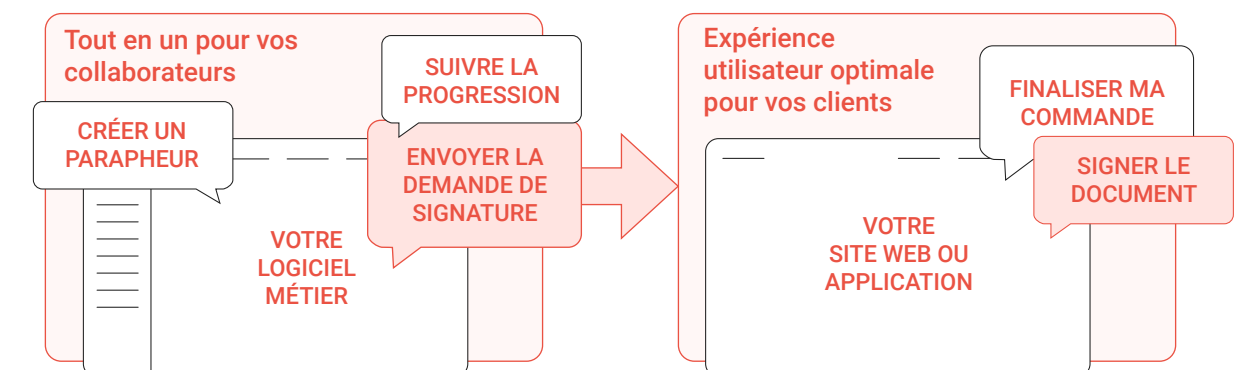


02

Signature électronique : comment l'intégrer dans son SI ?

Pour que la signature électronique soit utilisée de manière fluide et transparente et totalement intégrée aux processus métier, une phase d'intégration aux solutions documentaires est nécessaire. Explications.

L'intégration de la signature électronique doit être envisagée en deux phases.



En amont, il faut pouvoir signer ou faire signer directement depuis les applications que vous utilisez quotidiennement, à savoir, votre GED, une contrathèque, Salesforce, Sharepoint, SAP, les outils Microsoft et consorts.

Les collaborateurs pourront gérer la signature des contrats et autres (création, envoi, suivi...) **directement depuis leur logiciel métier habituel**.

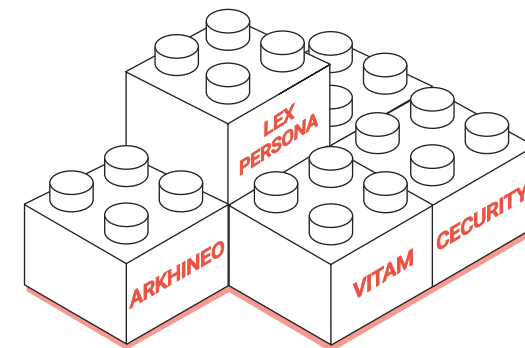
En évitant de multiplier les outils de travail, vous optimisez les tâches de vos employés et améliorez leur productivité.

Cette intégration offre par ailleurs une **meilleure expérience utilisateur**. Vos clients pourront signer leurs documents directement depuis votre site Internet ou application. Ils n'auront pas à attendre de recevoir les documents à signer par courriel ou courrier pour finaliser leur souscription à un service ou leur achat. Vous pourrez ainsi créer un **parcours client**, simplifié et 100% numérique. De plus, la signature étant immédiate, **le risque d'abandon d'achat est considérablement réduit**.

Si la solution métier n'est pas interopérable avec l'outil de signature électronique, l'organisation concernée doit effectuer un développement sur mesure pour appeler une API et pouvoir intégrer pleinement la signature électronique à l'application.

À l'inverse, si la solution métier est interopérable, il suffit d'utiliser le **connecteur** proposé. Certaines solutions métier proposent une marketplace avec différents connecteurs utilisables à la demande. C'est le cas par exemple de Salesforce. Et cela change complètement le parcours pour signer et faire signer un document. Grâce à ce connecteur, il est possible de lancer un workflow de signature depuis Salesforce. Sans lui, il aurait été nécessaire d'exporter les documents à faire signer, pour les intégrer dans un parapheur, via le portail et de créer le parcours de signature. Avec également un second parcours pour la récupération des documents signés.

Lex Persona propose des connecteurs avec les applications phares du marché et si besoin, peut aussi les développer.



En aval, il faut pouvoir déposer les documents signés et les fichiers de preuve associés dans un Système d'Archivage Electronique (SAE) ou un coffre-fort numérique.

Que deviennent les documents une fois signés ? Pour que ce parcours de signature soit sans couture, il convient de les déposer dans un SAE ou un coffre-fort numérique avec les fichiers de preuve associés. Et ce par le biais, là aussi, d'un connecteur.

L'API du programme Vitam peut, par exemple, être intégrée pour que les documents signés soient automatiquement déposés dans Vitam.

Aujourd'hui, Lex Persona s'intègre avec les solutions proposées par Cecurity Arkhineo, et Microsoft 365 (via Sharepoint), mais travaille également sur Vitam pour les acteurs publics.

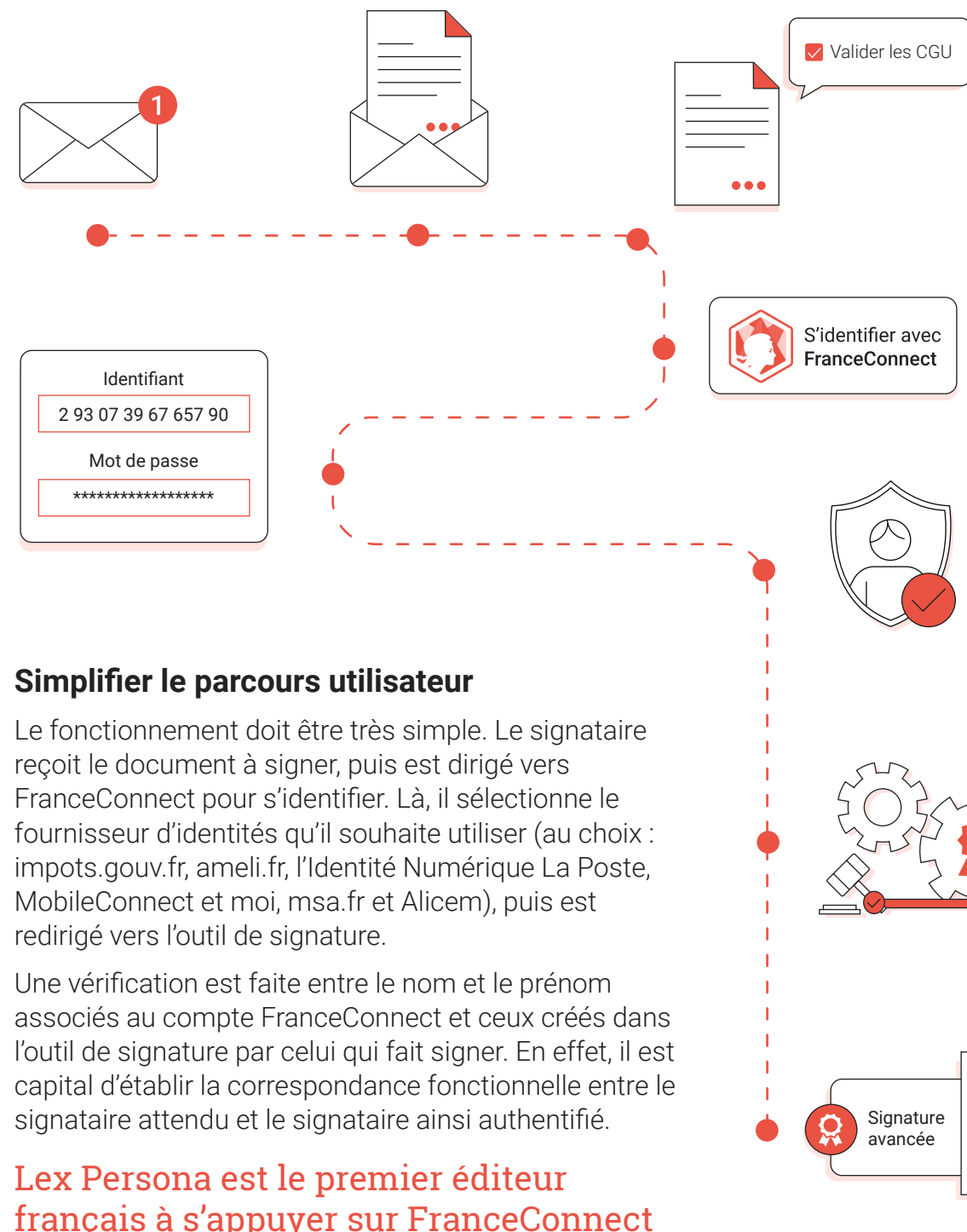
Au cahier des charges peuvent s'ajouter de nombreux éléments de personnalisation : demandes de signature avec le logo de l'entreprise, couleurs et typographies spécifiques, modification de l'apparence et des textes des emails reçus par les signataires, configuration en plusieurs langues, etc.

En intégrant la solution de signature électronique Lex Persona via API, vous pourrez automatiser vos processus, mais aussi personnaliser le service de signature en le mettant aux couleurs de votre entreprise.

L'intégration avec FranceConnect

Pour faire signer un document contractuel, il faut au préalable pouvoir identifier le signataire et être certain que c'est bien Madame XYZ qui signe. Pour identifier le signataire, plusieurs possibilités sont offertes, notamment celle de recourir à un fournisseur d'identité tiers comme FranceConnect, le fédérateur d'identités numériques créé par l'Etat. FranceConnect permet de sécuriser et simplifier la connexion à plus de 1000 services* en ligne. Et près de 35 millions de français* bénéficient d'un compte et peuvent ainsi gagner du temps dans leurs démarches en ligne.

*Sources : <https://franceconnect.gouv.fr/> au 8 mars 2022.



Simplifier le parcours utilisateur

Le fonctionnement doit être très simple. Le signataire reçoit le document à signer, puis est dirigé vers FranceConnect pour s'identifier. Là, il sélectionne le fournisseur d'identités qu'il souhaite utiliser (au choix : impots.gouv.fr, ameli.fr, l'Identité Numérique La Poste, MobileConnect et moi, msa.fr et Alicem), puis est redirigé vers l'outil de signature.

Une vérification est faite entre le nom et le prénom associés au compte FranceConnect et ceux créés dans l'outil de signature par celui qui fait signer. En effet, il est capital d'établir la correspondance fonctionnelle entre le signataire attendu et le signataire ainsi authentifié.

Lex Persona est le premier éditeur français à s'appuyer sur FranceConnect pour identifier l'auteur(e) d'une signature électronique. Cette signature bénéficie d'un niveau de sécurité avancé au sens du règlement eIDAS.



03

Avec quelle garantie en matière de sécurité et de confidentialité ?

La sécurité et la confidentialité s'immiscent de plus en plus dans la réglementation.

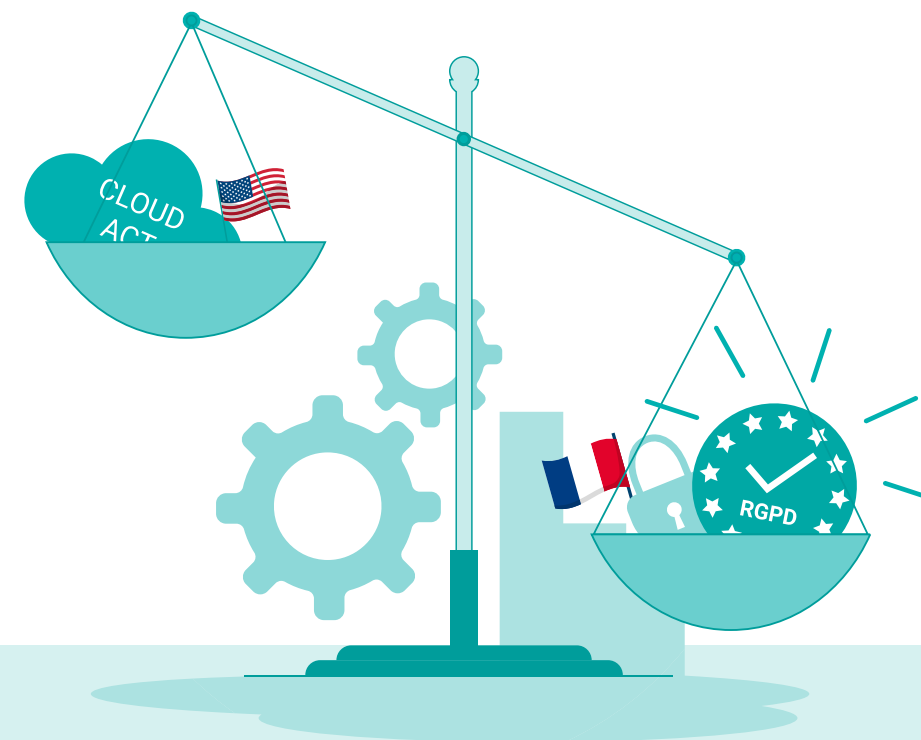
Règlement général pour la protection des données (RGPD), règlement eIDAS, loi pour une République numérique, projets de lois européennes relatives au Digital Services Act (DSA) et au Digital Market Act (DMA) : les réglementations qui impactent l'usage de la signature électronique ne manquent pas ! Jalon essentiel de la transformation numérique des organisations, cette technologies fait l'objet de nombreuses normes et législations que les éditeurs respectent à des niveaux différents.

Pour assurer la sécurité des données et leur confidentialité, Lex Persona ne laisse rien au hasard afin de permettre à ses utilisateurs de signer sans risque.

Un éditeur de signature électronique qui n'est pas soumis au Cloud Act

Outre-Atlantique, c'est le Cloud Act qui fait foi en matière de gestion des données. **Il stipule notamment que les fournisseurs de services établis sur le territoire américain doivent fournir les data de leurs clients du monde entier sur simple demande des instances de la justice américaine.** Une mesure qui soulève, bien sûr, de nombreuses problématiques liées à la protection de la vie privée et à laquelle sont soumis de nombreux éditeurs de signature électronique bien connus.

Basée à Troyes, Lex Persona ne dépend pas, de fait, du Cloud Act. L'entreprise va même plus loin, puisqu'elle ne travaille qu'avec des fournisseurs non soumis à cette législation, privilégiant les acteurs français. Dans cette même logique, Lex Persona est propriétaire des data centers qu'elle utilise, ces derniers étant basés en France.





Points de vigilance autour du RGPD

En tant que tiers de confiance considéré comme un sous-traitant par la réglementation, l'éditeur n'est pas responsable du traitement des données personnelles des utilisateurs de ses solutions. Cette obligation incombe donc aux clients de l'éditeur, qui ont recours à ses outils pour faire signer des documents.

Cependant, le fournisseur de signature électronique est obligé de conserver des données personnelles et données d'enregistrement permettant de vérifier l'identité d'un signataire (date de naissance, copie de pièce d'identité, etc.) pour une durée de 7 ans. Passé ce délai, ces informations sont supprimées ou anonymisées à la demande du client. Dans tous les cas, la durée de conservation et la nature des données archivées sont établies dès le début de la prestation avec le client. De même, la finalité du traitement réservé aux données doit systématiquement être précisée dans les Conditions générales d'utilisation de l'éditeur.

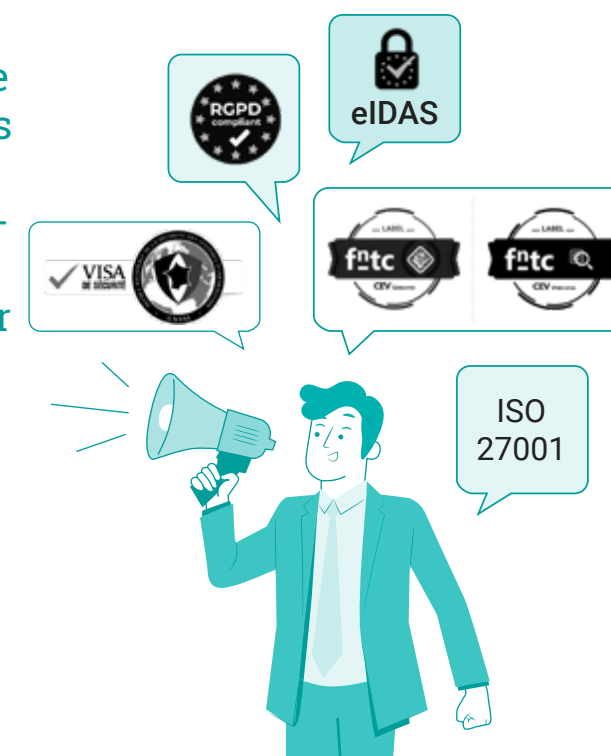
Non soumise au Cloud Act, Lex Persona est, en sus, très vigilante quant au respect du RGPD et précise bien les droits et devoirs respectifs de l'éditeur, de ses clients et de ses utilisateurs, que ce soit à travers ses contrats de service que ses conditions générales d'utilisation.

Les certifications, clef de voûte de la conformité et de la pérennité de vos signatures

Au-delà de répondre aux exigences réglementaires en vigueur, les dispositions entreprises par l'éditeur peuvent respecter les critères de différentes certifications et labels afin de garantir la fiabilité et la pérennité des signatures, des fichiers de preuves et des journaux produits. Ces certifications démontrent le bon respect des exigences de sécurité requises par certaines normes.

Parmi les certifications possibles, on retrouve la norme ISO 27001 (Management de la sécurité de l'information), ainsi que la très sélective liste de confiance de l'Union Européenne.

Lex Persona est ainsi auditée chaque année afin de confirmer qu'elle répond aux normes de différents organismes, notamment pour son service d'horodatage qualifié eIDAS, lui-même qualifié par l'ANSSI. Par ailleurs, elle offre la possibilité aux utilisateurs de signer avec des certificats automatiquement générés par une PKI, certifiée conforme à la norme ETSI EN 319-411 relative à la signature électronique. Elle est également labellisée 2D-Doc par la FNTC. À ce jour, l'API de signature électronique en ligne Lex Persona est la seule à être certifiée par l'ANSSI.



Intégrer une démarche « security by design »

À ces certifications peuvent s'ajouter d'autres initiatives pour garantir la sécurité et la maîtrise totale des processus liés à la signature électronique. La mise en place d'une architecture hybride mêlant un composant installé chez le client et une partie en SaaS chez l'éditeur, est, par exemple, un bon moyen de répondre aux organisations ayant des besoins de confidentialité très élevés (ministères, secteur de la défense, etc.).

Grâce à ce procédé hybride, seuls les signataires prennent connaissance des documents, qui ne passent jamais chez Lex Persona.

Le recours à des **cartes à puces** est, par ailleurs, parfaitement adapté aux **acteurs du secteur public**, qui disposent dès lors de certificats qualifiés de signature directement sur support physique, garantissant l'identité du signataire.

Cette solution, à l'instar des autres applications de l'éditeur, est produite en interne par Lex Persona, assurant une pleine maîtrise de celle-ci.



RETOUR D'EXPÉRIENCE

Coffreo intègre la signature électronique de Lex Persona dans ses processus de signatures électroniques de contrats et de documents

Proposant une plateforme de digitalisation de la relation avec les travailleurs temporaires, **Coffreo** a décidé en 2012 d'intégrer une solution de signature électronique à son propre outil. Pour ce faire, l'entreprise a choisi Lex Persona, aussi bien pour la simplicité d'intégration offerte par la solution que pour la possibilité de mettre en œuvre une signature électronique personnelle avec émission d'un certificat au nom de chaque salarié.

Avec pas moins de 30 millions de documents électroniques stockés, Coffreo est un acteur majeur de la transformation digitale des agences d'emploi et des entreprises ayant recours au travail temporaire et aux contrats courts. Un succès qui se ressent notamment dans le taux de signature des contrats de missions : les clients de Coffreo affichent en moyenne un **taux de 93 % de signature** contre 20 à 60 % en moyenne pour les acteurs utilisant un processus papier.

Le choix d'une solution performante et pleinement intégrée

Intégrer la signature électronique à ses processus était une évidence pour Coffreo, dont les 2 millions d'utilisateurs ont besoin de signer leurs contrats de travail de façon simple et rapide. Le choix de Lex Persona s'est imposé naturellement, guidé par 4 aspects principaux :

- la maîtrise technologique ;
- la possibilité de mettre en œuvre une signature électronique personnelle avec émission à la volée d'un certificat au nom de chaque salarié ;
- la simplicité d'intégration dans les sites et applications de Coffreo ;
- la compréhension des enjeux de l'entreprise.

« L'important dans un projet de signature électronique c'est qu'elle soit **intégrée à un workflow plus global pensé pour offrir la meilleure expérience possible à l'utilisateur** », rappelle Philippe Gasull, responsable de comptes chez Coffreo. « Notre objectif était de simplifier les processus et d'apporter de la souplesse et de la sécurité aux employeurs avec lesquels nous travaillons. L'intégration de Lex Persona y a largement contribué. »

Un parcours utilisateur rapide et fluide

En pratique, grâce au déploiement de la signature électronique Lex Persona au sein des outils Coffreo, les échanges se font à la fois **rapidement, efficacement et sans interruption**. Chaque intérimaire reçoit son contrat directement dans son coffre-fort numérique, le lit et coche une case. Un code d'authentification lui est alors envoyé par SMS afin d'intégrer la signature électronique. Coffreo reçoit ensuite des PDF des contrats et des informations complémentaires afin d'identifier chaque signataire.

« Un échange a lieu à ce moment-là entre Coffreo et Lex Persona et des informations telles que l'identité du signataire sont transmises à Lex Persona. Cela permet d'intégrer la signature électronique avec un certificat électronique personnel », détaille Philippe Gasull. « Chaque document est ensuite intégré à un coffre-fort où toutes les parties disposent d'un archivage à vocation probatoire qui intègre les signatures électroniques. »

Des bénéfices pour les employeurs comme pour les salariés

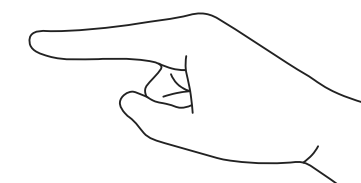
En plus d'être particulièrement simple, ce dispositif présente de nombreux avantages, tant pour les travailleurs que pour les employeurs clients de Coffreo.

Une agence d'intérim qui émet 200 contrats par mois observe ainsi en moyenne une économie de temps de 52 jours par an pour ses consultants.

Un gain de productivité important qui permet de se consacrer à des tâches à beaucoup plus forte valeur ajoutée.

« **Notre solution diminue la pénibilité pour nos clients et leur permet de gagner à la fois en simplicité et en sécurité.** », ajoute Philippe Gasull. « Il n'y a aucune raison objective pour qu'un salarié ne soit pas favorable au principe de la signature électronique de son contrat de travail ou d'un bulletin de paie », conclut-il.

EN SAVOIR PLUS





RETOUR D'EXPÉRIENCE

L'auto-facturation, un cas d'usage taillé pour le cachetage électronique

L'auto-facturaquoi ?

« Je te dirai ce que je te dois, merci, à bientôt ! » L'auto-facturation intervient fréquemment dans les grandes entreprises pour des transactions répétitives où il est plus arrangeant pour le « facturant » de laisser le « facturé » lui indiquer combien il lui doit. L'auto-facturation est une méthode de plus en plus courante qui la plupart du temps est réalisée numériquement.

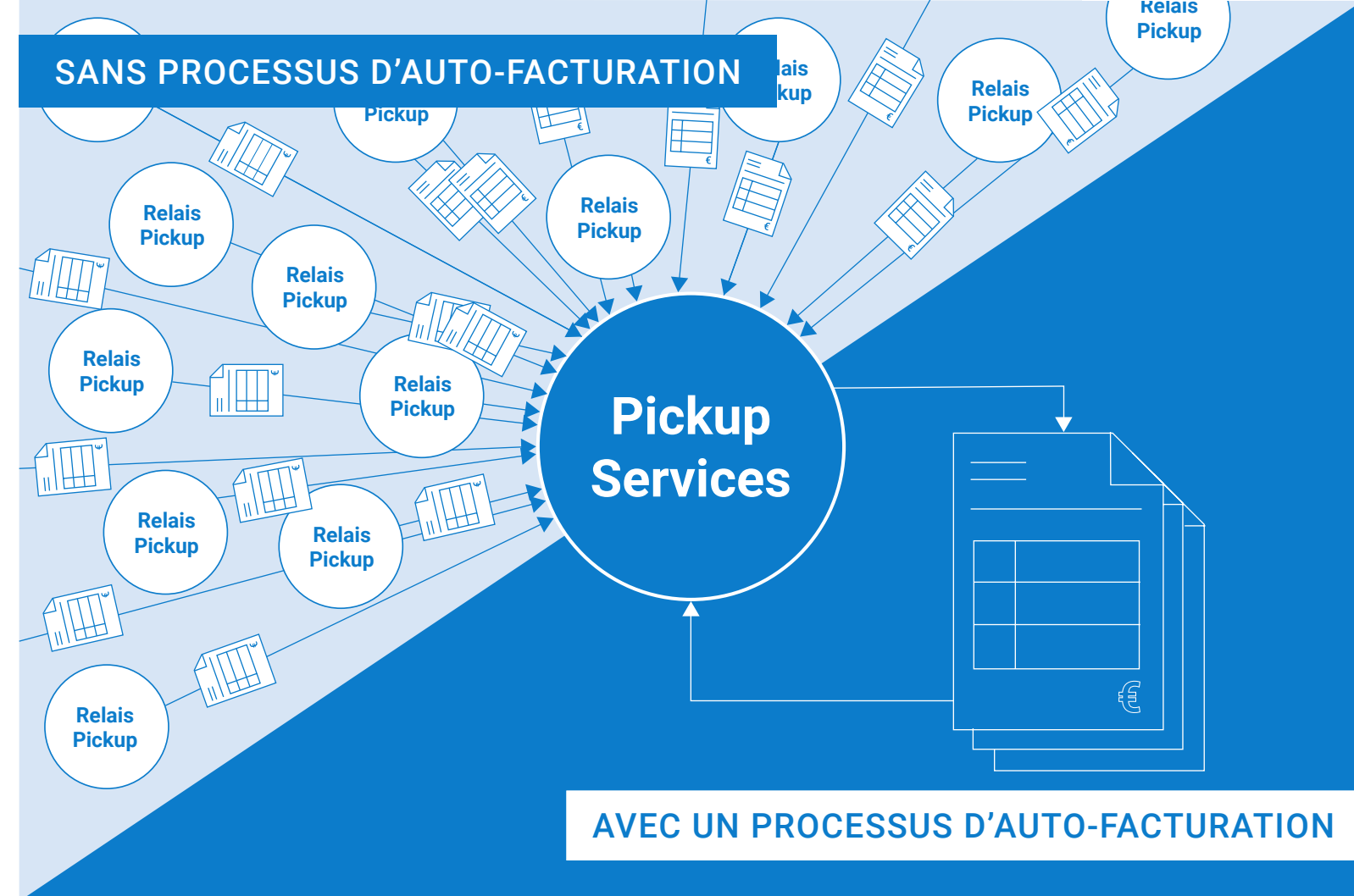
C'est là qu'intervient le cachetage électronique, pour éviter une falsification ou un malentendu. De manière plus générale, l'auto-facturation permet un gain en productivité pour les deux parties prenantes.

Pickup Services a intégré Lex Persona pour l'auto-facturation de ses points relais.

Epicerie, cordonniers, bureaux de tabac... Premier réseau du territoire, les relais Pickup Services sont désormais plus de **15 000** en France. Les jours de pointe, **600 000 colis sont livrés par jour** !

On imagine facilement le désordre si chacun établissait sa facture mensuelle à l'entreprise. Entre les pertes de temps, les litiges, et les différents formats, personne n'y trouverait son compte. C'est pourquoi l'entreprise a établi des mandats auprès des relais pour faire les factures mensuelles à leur place, et les envoyer par voie électronique.

Chaque mois, Pickup Services cache entre **13 et 15 000 auto-factures au format PDF**. On parle alors de **dématérialisation fiscale via un cachetage de niveau avancé, avec un certificat qualifié eIDAS**.



Un gain important en productivité grâce au cachetage électronique

Magali Raffoux, chef de projet Métier, et Jérôme Charpentier, chef de projet IT chez Pickup Services, témoignent :

« C'était pour nous un **gros projet** que de dématérialiser l'ensemble des auto-factures. Quelques mois après le lancement, presque **70% des points relais ont accepté de les recevoir par mail**, et donc cachetées électroniquement. »

Jusqu'à présent, les équipes support de chez Pickup Services se montrent satisfaites. Outre l'automatisation qui apporte une meilleure productivité, la mise en place d'une solution Lex Persona pour ce projet offre des gains financiers à court terme en raison des économies de papier et d'affranchissement réalisées.



RETOUR D'EXPÉRIENCE

Pour Aéroports de Paris, la signature électronique n'est plus en option

« La signature électronique fait l'unanimité au sein des équipes d'Aéroports de Paris, notamment grâce aux différentes fonctionnalités qu'elle englobe telles que la traçabilité des documents, l'authentification et la sécurité de ces derniers. La signature électronique fait partie intégrante de la GED de l'entreprise, elle permet de simplifier et raccourcir presque complètement les délais de signature de documents. Grâce à elle, Aéroports de Paris a pu gagner en efficacité, améliorer la collaboration entre ses différents services et ainsi moderniser sa gestion administrative. »

Témoignage de Dominique Etourneau, directeur des achats d'Aéroports de Paris concernant la signature électronique de Lex Persona.

En route vers la signature électronique

« Nous avons engagé un projet de dématérialisation de bout en bout, depuis l'appel à candidatures jusqu'à l'émission des commandes voire le paiement des factures. Et nous avons retenu la solution Lex Persona pour la signature électronique », confie Dominique Etourneau, directeur des achats d'Aéroports de Paris. Il ajoute que ce passage à la dématérialisation au sein du groupe s'est fait pas à pas, mais qu'en ce qui concerne la signature électronique tout a été réalisé en 3 mois. L'intégration de la signature électronique a effectivement été un changement majeur au sein du groupe Aéroports de Paris. « Nous étions tous convaincus de l'intérêt de la signature électronique pour l'entreprise. Ce qui nous a permis de systématiser la signature électronique : **ce n'est plus une option !** »

Un ROI immédiatement mesurable

La signature manuscrite de documents divers, tels que les factures ou les accords commerciaux, a toujours été un processus très long et donc très contraignant pour le groupe. En passant du support papier au numérique, la gestion est beaucoup plus simple. Les services n'ont plus besoin d'imprimer, de signer et de scanner le même document, comme l'explique Dominique Etourneau : « **La signature d'un contrat prenait en moyenne 2 à 3 semaines, alors qu'aujourd'hui c'est fait dans l'immédiat.** Cela veut dire que le fournisseur peut recevoir sa commande de suite, là où il devait attendre 3 semaines auparavant ».

Plus rapide, plus simple et surtout plus ergonomique, la signature électronique a renforcé la productivité du groupe et diminué drastiquement les délais d'attente :

« C'est un outil qui satisfait aux besoins de l'acheteur, du prescripteur mais aussi du fournisseur, puisqu'après un an d'utilisation, 90 % de nos contrats ont été signés de manière électronique, ce qui représente à peu près 700 marchés pour environ 500 fournisseurs. », ajoute-t-il.

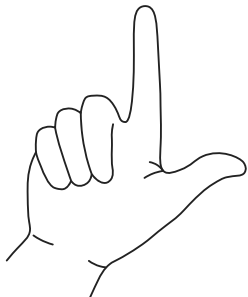
Traçabilité des validations et des signatures

La signature électronique renforce la sécurité et la confiance autour des documents.

« C'est un système qui nous permet de garantir la **traçabilité** et une certaine sécurité dans toutes nos transactions, poursuit le directeur achat. Ce dernier point est particulièrement important dans un environnement tel que le nôtre. Nous avons, en effet, des obligations d'archivage. Ainsi, une fois signés électroniquement, tous les documents sont versés dans un système d'archivage électronique. »

In fine, que ce soit via **smartphone, tablettes ou ordinateurs, la signature peut se faire en tout lieu et à tout moment**, protégée de surcroît par un système très sécurisé, ce qui facilite grandement les échanges commerciaux, RH et administratifs.

EN SAVOIR PLUS





Depuis 2005, Lex Persona s'est donnée pour mission de créer les conditions de la confiance dans les échanges dématérialisés à travers :

/ une expertise en matière d'intégrité, d'authenticité et de conformité des signatures électroniques ;

/ des logiciels et des services qui permettent de signer, faire signer et cacheter électroniquement tout type de document.

www.lex-persona.com

