

LAW RIGHT WEEKLY

Les nouveaux réflexes de confiance

Travail, patrimoine, identité : trois situations où vérifier change tout.



Illustrations conceptuelles créées avec l'aide de l'IA. Exemples fictifs. Information générale, pas un conseil personnalisé.

Dans ce numéro

01 Votre collaborateur utilise ChatGPT. Qui encadre les usages ?

02 Plus-values 2026 : avant le taux, la preuve

03 C'est sa voix. C'est son visage. Mais ce n'est pas votre patron.

Christophe Boeraeve · Law Right

Votre collaborateur utilise ChatGPT. Qui encadre les usages ?

Le risque peut commencer avant la réponse : au moment où un document quitte votre environnement.

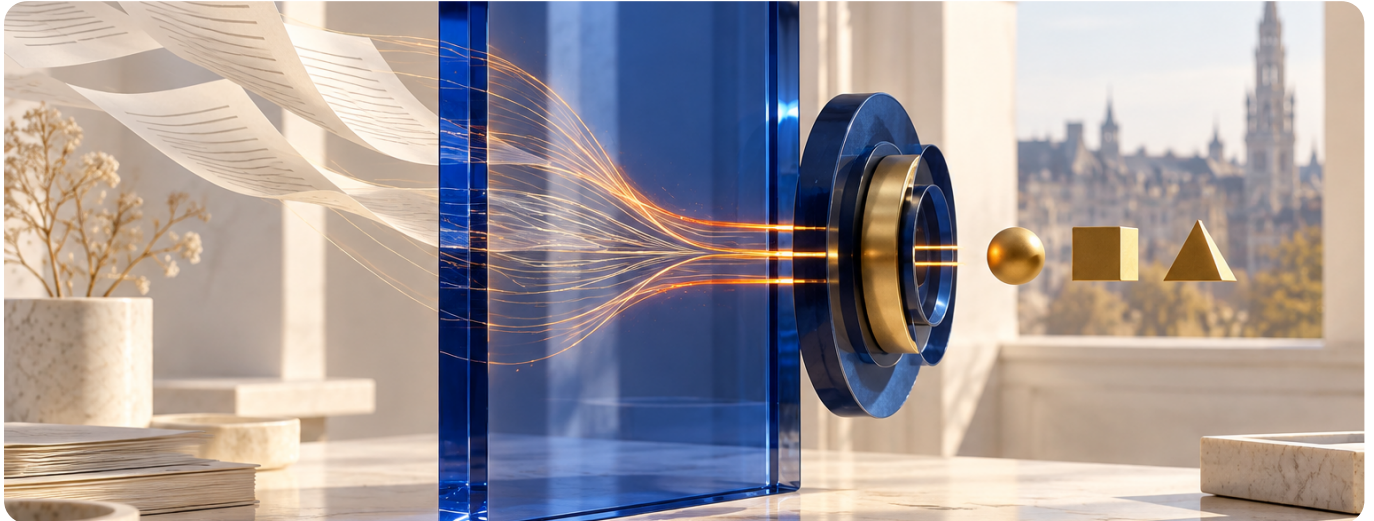


Illustration conceptuelle originale générée avec l'aide de l'IA pour Law Right ; aucune personne ni situation réelle représentée.

Scénario fictif. Une responsable commerciale transmet un contrat client à une IA pour préparer une négociation. Vingt minutes gagnées ; mais qui peut désormais conserver les informations, et pour quoi faire ? Le résumé paraît excellent. Le circuit suivi par les données reste, lui, à éclaircir.

L'actualité : une proposition nationale, une décision locale

Le 16 septembre 2026, Vanessa Matz a présenté une proposition de stratégie IA 2.0. Le communiqué en fait une base pour élaborer une stratégie nationale avec les entités fédérées, et non une nouvelle obligation générale pour les entreprises. Son ambition de maîtrise des usages pose pourtant une question immédiate aux PME et ASBL : qui autorise les outils, pour quels documents et avec quelles garanties ? [1]

Le 29 mai, l'APD avait souligné les risques liés aux conversations avec des chatbots : des échanges libres peuvent contenir des données très personnelles ; leur conservation doit être justifiée et leurs utilisations expliquées. C'est une communication du Service d'Inspection, pas une décision de sanction concernant notre scénario. [2]

Un compte professionnel n'est pas une immunité

Lorsque des données personnelles sont traitées, le RGPD exige notamment un fondement de licéité, une finalité déterminée, la minimisation et une protection appropriée. Le responsable doit pouvoir démontrer le respect de ces principes. Acheter une licence professionnelle ne constitue pas, à lui seul, cette démonstration. [3]

Examinez les rôles réels de l'organisation et du prestataire. Si celui-ci est sous-traitant, l'article 28 encadre la relation. Une analyse d'impact est requise lorsque le traitement envisagé est susceptible d'engendrer un risque élevé ; pas automatiquement pour toute correction de texte par IA. [4]

Toutes les informations confidentielles ne sont pas des données personnelles : prix négociés et projets commerciaux appellent aussi un examen des engagements de confidentialité. À l'inverse, retirer un nom ne garantit pas que le document ne permette plus d'identifier une personne. La question n'est donc pas seulement celle du logiciel : elle porte aussi sur le contenu, le contexte et la destination.

Le geste Law Right : cinq lignes avant le copier-coller

1. Écrivez une règle courte : outils autorisés, documents admis, données exclues, responsable de validation et canal de signalement. Prévoyez une solution praticable pour le collaborateur qui hésite.
2. Vérifiez les réglages, les accès, la conservation et la réutilisation éventuelle des données par le fournisseur. Si des données personnelles sont transférées hors Espace économique européen, vérifiez le mécanisme applicable et les garanties nécessaires. Cette méthode n'est pas un certificat de conformité belge. [5,6]
3. Gardez une personne responsable de la vérification du résultat. Testez la charte sur un document fictif avant de l'appliquer à des dossiers réels. Documentez les décisions utiles sans conserver inutilement le contenu confidentiel des échanges.

La bonne charte ne rassure pas seulement dans un classeur : elle aide à décider avant d'envoyer.

Sources et vérification

- [Vanessa Matz · 16.09.2026 · Proposition de stratégie IA 2.0](#)
- [APD/GBA · 29.05.2026 · Chatbots et protection des données](#)
- [RGPD/GDPR · Articles 5–6 · Texte reproduit par la CNIL](#)
- [RGPD/GDPR · Articles 24, 28, 32–35 · Texte reproduit par la CNIL](#)
- [CNIL · 18.07.2024 · Déployer une IA générative](#)
- [RGPD/GDPR · Chapitre V · Transferts internationaux · Texte reproduit par la CNIL](#)

[Retrouver la version web](#) ↗

Plus-values 2026 : avant le taux, la preuve

Le prix encaissé ne dit pas encore ce que vous avez gagné fiscalement. La valeur de départ, la catégorie de l'opération et les justificatifs peuvent changer le résultat.



Illustration conceptuelle originale générée avec l'aide de l'IA pour Law Right ; aucune personne ni situation réelle représentée.

Avant de demander combien vous paierez, demandez-vous ce que vous pouvez prouver.

Une réforme en vigueur, pas un taux universel

Cette présentation vise principalement les personnes physiques résidentes belges qui détiennent des titres dans leur patrimoine privé. Vous vendez des titres. Le prix apparaît sur votre compte. Mais ce montant ne dit pas encore ce que vous avez gagné fiscalement, ni ce qui vous restera après impôt. La question décisive n'est pas seulement « quel taux ? ». Elle est aussi : « quelle valeur de départ puis-je établir ? »

La loi du 6 avril 2026, publiée au Moniteur belge le 21 avril, a introduit un impôt sur les plus-values sur actifs financiers, avec effet au 1er janvier 2026. Nous ne sommes plus au stade des annonces gouvernementales. Il faut néanmoins distinguer l'impôt applicable depuis janvier du mécanisme légal de retenue à compter du 1er juin, assorti de règles transitoires. [1]

Quatre distinctions qui protègent le calcul

Qualifier avant de calculer. Le texte distingue les cessions internes, les participations d'au moins 20 % et le régime ordinaire. Un portefeuille privé, une participation dans sa société et un actif professionnel ne sont pas interchangeables. Une opération professionnelle ou étrangère à la gestion normale du patrimoine privé appelle une autre analyse. La formule « dix pour cent sur tout » est donc trompeuse. [1]

Établir le point de départ. Pour les actifs acquis avant 2026, la référence est en principe la valeur au 31 décembre 2025 : dernier cours de clôture de 2025 pour les titres cotés, méthodes légales spécifiques pour les titres non cotés. Sous les conditions du texte, le prix d'acquisition historique démontré peut être invoqué pour les cessions réalisées jusqu'au 31 décembre 2030. Ce n'est pas une liberté de choisir sa valorisation. [1]

La preuve compte réellement. Faute de données probantes sur la valeur d'acquisition, le prix reçu peut constituer la plus-value imposable. Un relevé, un contrat de souscription ou l'historique transmis lors d'une donation ne sont pas de simples archives. Pour les produits qu'elle décrit, l'Agence fédérale de la Dette insiste sur leur conservation lorsque des titres ont été donnés, hérités ou transférés. [1,2]

Distinguer retenue et impôt final. Dans le régime ordinaire, l'exonération annuelle atteint 10 000 euros pour 2026. La retenue par l'intermédiaire ne tient pas compte de cette exonération. Lorsqu'un précompte a été retenu, il faut demander son imputation et, le cas échéant, son remboursement via la déclaration pour bénéficier de l'exonération, avec justificatifs disponibles. Les moins-values ne se compensent pas librement : même contribuable, même période imposable et même catégorie légale. [1,2]

Le dossier à réunir avant de vendre

1. Retrouvez les preuves d'achat, dates, quantités, devises et relevés au 31 décembre 2025. Pour des titres reçus, conservez aussi l'historique pertinent du donateur ou du défunt.
2. Rassemblez les opérations de 2026, les gains et pertes par catégorie, les décomptes de retenue et les attestations. Un transfert de banque ne devrait pas effacer votre dossier documentaire.
3. Avant une cession importante, faites vérifier le régime applicable, les liens entre vendeur et acheteur et la méthode de valorisation. Cette checklist n'est ni une simulation fiscale ni un conseil de vendre ; elle prépare un examen adapté à votre situation.

La bonne préparation fiscale commence par un dossier vérifiable, pas par un pourcentage rassurant.

Sources et vérification

- [Loi du 6 avril 2026 — art. 3, 10–11, 14, 22, 28 et 34–35 ; CIR 92, art. 90, 96/2, 102, 261 et 307](#)
- [Agence fédérale de la Dette — FAQ, préambule et questions 3.2 et 5.1 \(produits de l'Agence\)](#)

[Retrouver la version web](#) ↗

C'est sa voix. C'est son visage. Mais ce n'est pas votre patron.

Pour un paiement sensible, une apparence familière ne remplace pas un circuit de validation.



Illustration conceptuelle originale générée avec l'aide de l'IA pour Law Right ; aucune personne ni situation réelle représentée.

Scénario fictif. Un vendredi, une comptable reçoit une demande urgente de virement. Un appel vidéo paraît confirmer l'instruction de la direction. Le compte est nouveau, mais l'opération doit rester confidentielle. Faut-il croire le visage familier ou suivre la procédure habituelle ?

Un risque documenté, pas une nouvelle alerte inventée

Le 24 janvier 2026, le parquet fédéral et le Centre pour la Cybersécurité Belgique ont alerté sur des escroqueries usurpant l'identité du Roi et d'autres personnalités. Des chefs d'entreprise figuraient parmi les personnes visées. Le communiqué parle d'images vidéo vraisemblablement générées par IA : ce n'est pas une confirmation technique publique de chaque séquence. [1]

La fraude ne repose pas toujours sur un outil spectaculaire. Safeonweb décrit aussi une préparation : collecte d'informations sur l'organisation, usurpation d'une personne de confiance, puis demande d'argent ou de données. L'urgence et la confidentialité servent à contourner les contrôles. Une vidéo convaincante renforce l'apparence ; elle ne valide pas l'opération. [2,3]

Reconnaître, autoriser et prouver : trois questions différentes

Une demande crédible n'est pas nécessairement authentique. Même lorsqu'une identité est vérifiée, il faut encore établir si l'opération est autorisée dans le circuit de l'organisation. Nous proposons ici une distinction pratique : reconnaître une personne, vérifier son instruction et confirmer les pouvoirs nécessaires sont trois étapes à ne pas confondre.

Si l'incident révèle aussi une violation de données personnelles, une analyse RGPD distincte s'impose. Selon l'article 33, le responsable du traitement notifie l'autorité dans les meilleurs délais et si possible sous 72 heures après en avoir pris connaissance, sauf si la violation n'est pas susceptible d'engendrer un risque pour les droits et libertés. Le sous-traitant avertit le responsable sans délai indu. L'information des personnes relève du risque élevé et des conditions de l'article 34. Tout faux appel ne déclenche donc pas automatiquement une notification RGPD. [4]

Ni la récupération des fonds ni un remboursement ne peuvent être promis à partir du seul récit d'une usurpation. Leur examen nécessite les faits, les opérations concernées et le régime applicable. Prévenir, signaler et conserver les éléments utiles reste possible sans préjuger cette analyse.

Le geste Law Right : un deuxième chemin avant de payer

1. Rappelez par un numéro déjà connu et obtenu indépendamment du message suspect. Faites vérifier tout nouveau bénéficiaire ; maintenez la validation prévue pour les paiements sensibles. La discrétion demandée ne doit pas supprimer le contrôle habituel. [2]
2. Si le virement est parti, contactez immédiatement la banque et les responsables internes. Signalez la fraude à la police selon la situation. L'urgence de réagir n'équivaut pas à une garantie de récupération. [2,3]
3. Préservez de façon sécurisée les éléments utiles au traitement de l'incident : messages originaux, horaires, coordonnées et références de paiement. Organisez la collecte avec le responsable compétent ; ne diffusez pas largement les données ou pièces sensibles.

Même face à un supérieur apparent, chacun doit pouvoir suspendre pour vérifier.

Sources et vérification

- [CCB · 24.01.2026 · Usurpation de personnalités publiques](#)
- [Safeonweb · Fraude au CEO : prévention et réaction](#)
- [Safeonweb at Work · Fraude au CEO](#)
- [RGPD/GDPR · Articles 33–34 · Notification des violations](#)

[Retrouver la version web](#) ↗

Trois fiches à emporter

01 · Travailler

- Écrivez une règle courte : outils autorisés, documents admis, données exclues, responsable de validation et canal de signalement. Prévoyez une solution praticable pour le collaborateur qui hésite.
- Vérifiez les réglages, les accès, la conservation et la réutilisation éventuelle des données par le fournisseur. Si des données personnelles sont transférées hors Espace économique européen, vérifiez le mécanisme applicable et les garanties nécessaires. Cette méthode n'est pas un certificat de conformité belge. [5,6]
- Gardez une personne responsable de la vérification du résultat. Testez la charte sur un document fictif avant de l'appliquer à des dossiers réels. Documentez les décisions utiles sans conserver inutilement le contenu confidentiel des échanges.

02 · Documenter

- Retrouvez les preuves d'achat, dates, quantités, devises et relevés au 31 décembre 2025. Pour des titres reçus, conservez aussi l'historique pertinent du donateur ou du défunt.
- Rassemblez les opérations de 2026, les gains et pertes par catégorie, les décomptes de retenue et les attestations. Un transfert de banque ne devrait pas effacer votre dossier documentaire.
- Avant une cession importante, faites vérifier le régime applicable, les liens entre vendeur et acheteur et la méthode de valorisation. Cette checklist n'est ni une simulation fiscale ni un conseil de vendre ; elle prépare un examen adapté à votre situation.

03 · Vérifier

- Rappelez par un numéro déjà connu et obtenu indépendamment du message suspect. Faites vérifier tout nouveau bénéficiaire ; maintenez la validation prévue pour les paiements sensibles. La discrétion demandée ne doit pas supprimer le contrôle habituel. [2]
- Si le virement est parti, contactez immédiatement la banque et les responsables internes. Signalez la fraude à la police selon la situation. L'urgence de réagir n'équivaut pas à une garantie de récupération. [2,3]
- Préservez de façon sécurisée les éléments utiles au traitement de l'incident : messages originaux, horaires, coordonnées et références de paiement. Organisez la collecte avec le responsable compétent ; ne diffusez pas largement les données ou pièces sensibles.

Un échange humain

cboeraeve@law-right.com · [+32 467 111 777](tel:+32467111777) / WhatsApp

Cette édition a été préparée avec l'assistance de l'IA pour la recherche, la rédaction, la traduction, les illustrations et le code. Information générale ; publication sous la responsabilité éditoriale de Christophe Boeraeve. Les exemples sont fictifs et les schémas ne calculent aucun résultat juridique.