005 / EN
23 September 2026

LAW RIGHT WEEKLY

# New habits of trust

Work, wealth, identity: three situations where verification makes a difference.

Conceptual illustrations created with AI assistance. Fictional examples. General information, not personalised advice.

## In this issue

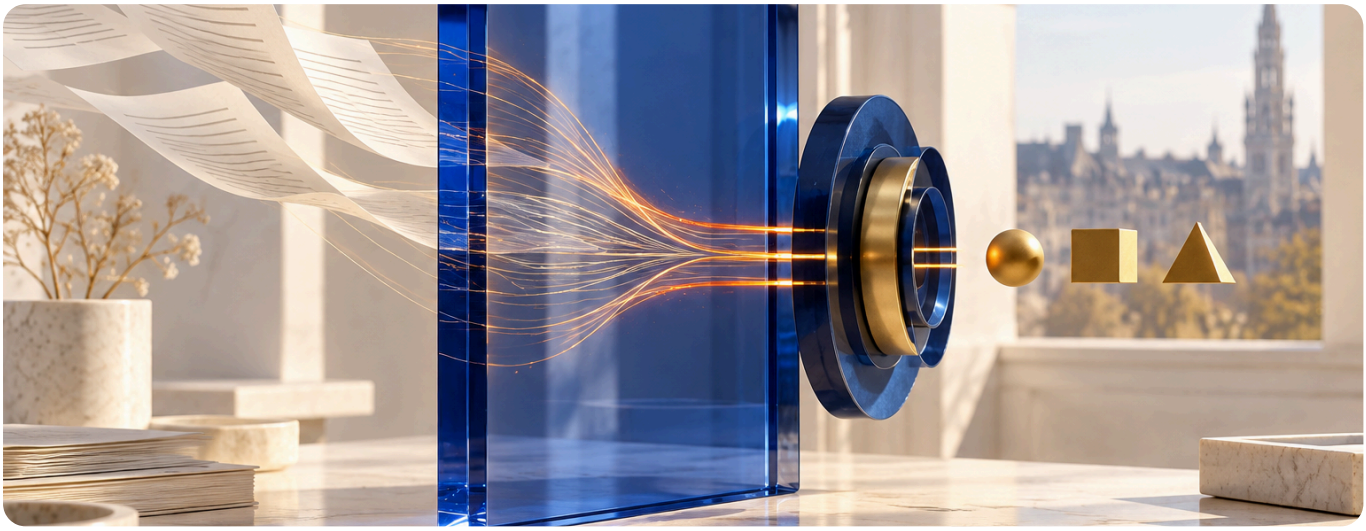


**Christophe Boeraeve · Law Right**

DOSSIER 01 / DATA PROTECTION · CONTRACT LAW · EMPLOYMENT LAW

# Your employee uses ChatGPT. Who sets the rules?

The risk may begin before the answer: when a document leaves your own environment.



Original conceptual illustration generated with AI assistance for Law Right; no real person or event depicted.

> Fictional scenario. A sales manager gives an AI assistant a client contract to prepare for negotiations. Twenty minutes saved. But who can now retain that information, and for what purposes? The summary looks excellent. The route taken by the data remains unclear.

## The news: a national proposal, a local decision

On 16 September 2026, Vanessa Matz presented a proposed AI Strategy 2.0. The announcement describes a basis for developing a national strategy with Belgium's federated entities, not a new general obligation on businesses. Its ambition to retain control of AI use nevertheless poses a practical question for SMEs and non-profits: who approves tools, for which documents and with which safeguards? [1]

On 29 May, Belgium's Data Protection Authority highlighted risks in chatbot conversations. Free-text exchanges can include highly personal data; retention must be justified and uses explained. This was an Inspectorate communication, not a sanction decision concerning the fictional scenario above. [2]

01 / WORK

# A business account is not legal immunity

Where personal data are processed, the GDPR requires, among other things, a lawful basis, a defined purpose, data minimisation and appropriate protection. The controller must be able to demonstrate compliance. Purchasing a business licence does not, by itself, provide that demonstration. A product label cannot establish what actually happens to a particular document. [3]

Examine the organisation's and provider's actual roles. If the provider acts as a processor, Article 28 governs that relationship. A data protection impact assessment is required where the intended processing is likely to result in a high risk, not automatically whenever AI corrects a piece of text. [4]

Not all confidential information is personal data. Negotiated prices and business plans also require attention to contractual confidentiality commitments. Conversely, removing a name does not necessarily prevent identification through the remaining details. The assessment concerns the software, but also the content, context and destination of the information.

### The Law Right approach: five rules before pasting

1. Write a short rule identifying approved tools, permitted documents, excluded data, the person responsible for approval and the incident-reporting channel. Give employees a workable route when they are unsure.
2. Check settings, access, retention and possible reuse by the provider. If personal data are transferred outside the European Economic Area, verify the applicable mechanism and necessary safeguards. This approach is not a Belgian compliance certificate. Verify your organisation's actual configuration, not just marketing language. [5,6]
3. Keep a person responsible for checking the output. Test the policy with a fictional document before applying it to real files. Record useful decisions without unnecessarily retaining confidential conversation content. A policy should make safer work possible, not merely relocate uncertainty to the employee.

**A good AI policy does more than reassure in a folder. It helps people decide before they send.**

## Sources and verification


- 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


Explore the web edition ↗

DOSSIER 02 / TAX LAW · PROPERTY LAW · LAW OF EVIDENCE

# Capital gains in 2026: evidence before the rate

The sale proceeds are not the same as your taxable gain. The starting value, the category of transaction and the supporting records can change the result.

Original conceptual illustration generated with AI assistance for Law Right; no real person or event depicted.

> Before asking how much you will pay, ask what you can prove.

## An enacted reform, not a universal rate

This overview primarily concerns Belgian-resident individuals holding securities as part of their private assets. You sell securities. The proceeds appear in your account. Yet that amount does not tell you your taxable gain or what you will retain after tax. The decisive question is not simply: “What rate applies?” It is also: “What starting value can I establish?” This article concerns Belgian tax law.

The Act of 6 April 2026, published in the Belgian Official Gazette on 21 April, introduced a tax on capital gains on financial assets, taking effect from 1 January 2026. This is no longer merely a government announcement. However, the tax applying since January must be distinguished from the statutory withholding mechanism starting on 1 June, which is subject to transitional rules. [1]

02 / DOCUMENT

# Four distinctions that protect the calculation

Classify before calculating. The legislation distinguishes internal transfers, shareholdings of at least 20% and the ordinary regime. A private portfolio, a holding in your own company and a business asset are not interchangeable. A professional transaction or one outside the normal management of private assets requires a different analysis. “Ten per cent on everything” is therefore misleading. [1]

Establish the starting value. For assets acquired before 2026, the reference is generally their value on 31 December 2025: the last closing price of 2025 for listed securities, and specific statutory valuation methods for unlisted securities. Subject to the statutory conditions, a proven historical acquisition value may be relied upon for disposals up to 31 December 2030. This does not permit a free choice of valuation. [1]

Evidence genuinely matters. Without reliable evidence of the acquisition value, the proceeds received may constitute the taxable capital gain. A statement, subscription agreement or transaction history passed on with a gift is therefore more than an archive. For the products it describes, the Belgian Debt Agency stresses the importance of preserving these records when securities have been gifted, inherited or transferred. [1,2]

Separate withholding from the final tax. Under the ordinary regime, the annual exemption is €10,000 for 2026. Withholding by the intermediary does not take that exemption into account. Where withholding tax has been deducted, claiming the exemption requires a request for credit and, where applicable, a refund through the tax return, with supporting documents available. Losses cannot be offset without limits: they must concern the same taxpayer, the same taxable period and the same statutory category. [1,2]

### The file to assemble before selling

1. Locate purchase records, dates, quantities, currencies and statements showing values on 31 December 2025. For securities received from someone else, preserve the relevant history of the donor or deceased owner too.
2. Bring together your 2026 transactions, gains and losses by category, withholding statements and certificates. Moving to another bank should not mean losing the records needed to establish your position.
3. Before a substantial disposal, have the applicable regime, the connections between seller and buyer, and the valuation method reviewed. This checklist is neither a tax simulation nor advice to sell. It prepares the ground for an assessment tailored to your circumstances.

**Sound tax preparation starts with a verifiable file, not a reassuring percentage.**

## Sources and verification


- Act of 6 April 2026 — Arts 3, 10–11, 14, 22, 28 and 34–35; Belgian Income Tax Code 1992, Arts 90, 96/2, 102, 261 and 307 (French text)
- Belgian Debt Agency — FAQ, introduction and questions 3.2 and 5.1 (Agency products; French text)


Explore the web edition ↗

DOSSIER 03 / CYBERSECURITY · DATA PROTECTION · LIABILITY

# It is their voice. It is their face. But it is not your boss.

For a sensitive payment, a familiar appearance cannot replace an approval process.

Original conceptual illustration generated with AI assistance for Law Right; no real person or event depicted.

> Fictional scenario. On a Friday, an accountant receives an urgent transfer request. A video call appears to confirm management's instruction. The bank account is new, but the transaction must remain confidential. Should she trust the familiar face or follow the usual procedure?

## A documented risk, not a newly invented alert

On 24 January 2026, Belgium's federal prosecutor and Centre for Cybersecurity warned about scams impersonating the King and other public figures. Business leaders were among those targeted. The announcement describes video images as likely AI-generated. That wording matters: it is not public forensic confirmation of every individual recording. [1]

The fraud does not always depend on spectacular technology. Safeonweb also describes preparatory research into an organisation, impersonation of a trusted person, and requests for money or information. Urgency and secrecy are used to bypass controls. Convincing video strengthens an appearance; it does not authorise a transaction. [2,3]

03 / VERIFY

# Recognition, authority and evidence are different questions

A credible request is not necessarily authentic. Even if an identity is verified, the transaction must still be approved through the organisation’s decision-making process. Our practical approach separates three steps: recognising the person, checking the instruction and confirming the necessary authority. Success at one step should not silently replace the others.

If the incident also reveals a personal data breach, a separate GDPR assessment is required. Under Article 33, the controller notifies the supervisory authority without undue delay and where feasible within 72 hours of awareness, unless the breach is unlikely to result in a risk to rights and freedoms. The processor informs the controller without undue delay. Informing affected individuals involves a high-risk threshold and the conditions of Article 34. Not every impersonation call therefore automatically triggers a GDPR notification. [4]

Neither recovery of funds nor reimbursement can be promised merely because impersonation is alleged. The facts, transactions and applicable legal framework require examination. Prevention, reporting and securing relevant information can proceed without prejudging that assessment. An urgent operational response and a legal conclusion are not the same thing.

### The Law Right approach: a second route before paying

1. Call back using an established number obtained independently of the suspicious message. Have any new beneficiary checked and retain the normal approval process for sensitive payments. A request for discretion must not remove the usual control. [2]
2. If the transfer has already been made, contact the bank and internal responsible persons immediately. Report the fraud to the police as appropriate. Acting quickly matters, but does not guarantee that the money can be recovered. [2,3]
3. Secure relevant incident material: original messages, times, contact details and payment references. Coordinate its preservation with the appropriate person. Avoid circulating sensitive evidence unnecessarily, even when colleagues understandably want to know what happened.

**Even when a request appears to come from a superior, people must be able to pause and verify.**

## Sources and verification


- 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


Explore the web edition ↗

# Three practical checklists

### 01 · Work

□ Write a short rule identifying approved tools, permitted documents, excluded data, the person responsible for approval and the incident-reporting channel. Give employees a workable route when they are unsure.

□ Check settings, access, retention and possible reuse by the provider. If personal data are transferred outside the European Economic Area, verify the applicable mechanism and necessary safeguards. This approach is not a Belgian compliance certificate. Verify your organisation's actual configuration, not just marketing language. [5,6]

□ Keep a person responsible for checking the output. Test the policy with a fictional document before applying it to real files. Record useful decisions without unnecessarily retaining confidential conversation content. A policy should make safer work possible, not merely relocate uncertainty to the employee.

### 02 · Document

□ Locate purchase records, dates, quantities, currencies and statements showing values on 31 December 2025. For securities received from someone else, preserve the relevant history of the donor or deceased owner too.

□ Bring together your 2026 transactions, gains and losses by category, withholding statements and certificates. Moving to another bank should not mean losing the records needed to establish your position.

□ Before a substantial disposal, have the applicable regime, the connections between seller and buyer, and the valuation method reviewed. This checklist is neither a tax simulation nor advice to sell. It prepares the ground for an assessment tailored to your circumstances.

### 03 · Verify

□ Call back using an established number obtained independently of the suspicious message. Have any new beneficiary checked and retain the normal approval process for sensitive payments. A request for discretion must not remove the usual control. [2]

□ If the transfer has already been made, contact the bank and internal responsible persons immediately. Report the fraud to the police as appropriate. Acting quickly matters, but does not guarantee that the money can be recovered. [2,3]

□ Secure relevant incident material: original messages, times, contact details and payment references. Coordinate its preservation with the appropriate person. Avoid circulating sensitive evidence unnecessarily, even when colleagues understandably want to know what happened.

## Human assistance

cboeraeve@law-right.com · +32 467 111 777 / WhatsApp

This edition was prepared with AI assistance for research, drafting, translation, illustrations and code. General information; published under the editorial responsibility of Christophe Boeraeve. Examples are fictional and diagrams do not calculate legal outcomes.