VAN BAEL & BELLIS

# Law on Private Investigations | A Stricter Framework for Internal Investigations

On 6 December 2024, the long-awaited Law of 18 May 2024 governing private investigations (*Wet van 18 mei 2024 tot regeling van de private opsporing / Loi du 18 mai 2024 réglementant la recherche privée* - the **Law**) was published in the Belgian Official Journal. The Law establishes a comprehensive framework for organisations conducting internal investigations (e.g. in relation to suspected fraudulent or wrongful acts committed by their employees).

The Law came into force on **16 December 2024.** As it establishes only a general framework, its implementation will depend on a series of Royal Decrees. At the time of publication of this newsflash, none of these Royal Decrees have been published.

## 1. CONTEXT

The Law **replaces** the Law of 10 July 1991 regulating the private detective profession (*Wet tot regeling van het beroep van privé-detective / Loi organisant la profession de détective privé*), which required modernisation to reflect technological advancements, privacy concerns, and the expansion of the private detective profession to fraud auditors, forensic accountants and various other professionals.

The Law mainly addresses the gap that emerged between public investigations (such as police-led criminal investigations) and private investigations in terms of investigatory powers and techniques. It also seeks to enhance privacy and other fundamental rights of private individuals involved.

This newsflash outlines the scope of the Law and its key implications for any organisation with an in-house investigation team conducting internal investigations.

## 2. EXTENDED SCOPE

The Law has a broad scope and applies to **all private investigation activities** carried out by external investigators as well as company in-house investigation teams. Its scope is limited to activities that involve the collection of information about private individuals in the framework of private investigations. These can involve a private investigator or a private individual (e.g. an employee in the HR department) who provides this information to a principal (e.g. an employer) to **protect its interests in an ongoing conflict** or a **potential conflict** or in an investigation aiming to trace missing persons or locate lost or stolen goods.

Certain activities are explicitly **excluded from the scope** of the Law. The most significant exceptions are:

- audits which are not aimed at investigating undesirable behaviour (financial audits);
- cybersecurity monitoring to ensure system integrity;
- activities conducted by professionals such as notaries, lawyers, journalists or company auditors;

- insurance claim investigations; and
- investigations conducted under a legal obligation, such as those performed by (i) external prevention advisors in the context of psychosocial risks at work such as violence, harassment and sexual harassment, or (ii) whistleblowing officers handling a reported breach under the applicable whistleblowing legislation.

## 3. REQUIREMENTS FOR IN-HOUSE INVESTIGATION TEAMS

### 3.1. OBLIGATIONS REGARDING LICENSING AND IDENTIFICATION CARDS

Organisations must obtain a five-year, renewable **licence** from the Ministry of Home Affairs to operate an in-house investigation team.

**The licence** must be **disclosed** on all documents prepared in the framework of the investigation. It can be **revoked** in the event of non-compliance.

Additionally, the Law lays down **specific requirements** for the members of in-house investigation teams, managers of these teams, and members of the board of directors. These include specific training requirements and the completion of a profile background check carried out by the Ministry of Home Affairs. Obligations to adhere to strict compatibility rules and to comply with security requirements also apply. If these conditions are met, applicants are issued an **identification card** from the Ministry of Home Affairs.

As an exception, members of in-house HR teams conducting an incident investigation (*incidentenonderzoek / enquête d'incidents*) concerning employees are **exempt from the obligations regarding licensing and identification cards**. All the other formalities as mentioned below nevertheless apply. An incident investigation can for example relate to a one-off investigation as to whether an employee violated internal policies, in the context of envisaged dismissal for serious cause, by conducting interviews and/or analysing camera footage.

### 3.2. RULES FOR CONDUCTING AN INTERNAL INVESTIGATION

The Law specifies the **methods, procedures and rules of conduct** to be followed when conducting an internal investigation.

#### (i) GDPR Compliance

All **data processing** must comply with the General Data Protection Regulation (**GDPR**) and the Belgian Data Protection Law. The Law designates organisations and in-house investigation teams as data controllers within the meaning of the GDPR in respect of the data they collect, analyse, process, store, and include in their investigation reports.

The in-house investigation team must include a **designated data protection officer** (**DPO**) who must ensure compliance with data protection laws and monitor the handling of personal information during investigations. This can be an internal member of the in-house investigation team or an external consultant.

Furthermore, the Law **prohibits investigations in certain areas** (e.g. political views, religion, genetic data, racial or ethnic origin, health information, ongoing court cases, etc.), subject to some exceptions.

The **confidentiality** of all personal data collected during a private investigation must be ensured at all times and used solely for the purposes of fulfilling the specific assignment.

**(ii) Assignment Register and Investigation Report**

The in-house investigation team must retain an **assignment register** including specific mandatory elements (e.g. description of the assignment/investigation, the start and end date of the investigation, etc.) which must be retained for five years.

No later than one month after completion of the investigation, the in-house investigation team must provide the organisation with a **written investigation report**. This report should be signed by all members of the in-house investigation team and be used only to defend the legitimate interests of the principal / employer.

Within 30 days of receiving the final report, the organisation must notify the in-house investigation team in writing **whether further action will be taken**.

**(iii) Written Internal Policy**

Organisations must transparently outline the circumstances under which an investigation may be initiated and the specific investigation methods in a **written internal policy.** This policy can be a stand-alone document or can be integrated into work rules or a collective labour agreement.

The works council, or failing such body any other employee representative bodies, should also be consulted in advance prior to the implementation of the policy.

In the absence of a written policy, the Law prohibits the investigations of employees.

Organisations have a **period of two years** from the entry into force of the Law to comply with this obligation. If no policy is adopted by this time, all internal investigations and their findings will be null and void.

**(iv) Specific Rules for Interviews**

**An interview** may be conducted only with the **prior written consent** of the interviewee, who must have been **proactively informed** of the purpose of the interview and other mandatory elements.

During interviews, interviewees have **the right to be represented** by a person of their choice, such as a lawyer or a trade union representative.

**A written report** must be made of the interview, including the details of all involved parties and confirmation that all legal requirements were met.

## 4. COMPLIANCE

**Compliance** with the Law is **overseen by** the Data Protection Authority (*de Gegevensbeschermingsauthoriteit / l'Autorité de protection de données*), police services, and specific public servants / inspectors.

It is important to note that **inspectors have far-reaching monitoring powers** and that they can freely enter workplaces where they have reasonable grounds to believe that violations of the Law are taking place.

Finally, **courts also hold oversight authority** and will evaluate whether evidence from private investigations was obtained in compliance with the provisions of the Law. Evidence obtained in the framework of non-compliant internal investigations may be found inadmissible.

**Sanctions for non-compliance** can also be imposed. Potential sanctions consist of (i) a warning, (ii) an amicable settlement (30% of the administrative fine), and (iii) an administrative fine ranging from EUR 100 to EUR 25,000 (with more severe fines in the event of repeated non-compliance).

The Data Protection Authority may also impose sanctions for violations of data protection provisions under the GDPR.

## 5. WHAT IS NEXT?

The framework established by the Law will be further implemented and refined through Royal Decrees. As a result, the timing and specifics of the Law's requirements are as yet unclear.

**VBB** would in the meantime be **pleased to assist with**:

- providing a detailed analysis of specific steps your organisation should undertake to comply with the Law;
- drafting the required internal policy and/or updating work rules; and
- addressing any other inquiry that you may have about the Law.

VAN BAEL & BELLIS

BRUSSELS
Glaverbel Building
Chaussée de La Hulpe 166
B-1170 Brussels, Belgium
Phone : +32 (0)2 647 73 50
Fax : +32 (0)2 640 64 99

GENEVA
26, Bd des Philosophes
CH-1205 Geneva
Switzerland
Phone : +41 (0)22 320 90 20
Fax : +41 (0)22 320 94 20

LONDON
Holborn Gate
330 High Holborn
London, WC1V 7QH
United Kingdom
Phone : +44 (0)20 7406 1471