Report on the Review of the provisions pertaining to the disclosure of an officer's residential addresses having regard to company transparency requirements and GDPR

September 2025

Contents

1. Scope

The Company Law Review Group (the "**Review Group**") was tasked in its 2024-2026 Work Programme with reviewing the provisions and process pertaining to the disclosure of an Officer's residential addresses having regard to company transparency requirements and GDPR.

This issue has been brought to the attention of the Review Group by a submission from the Law Society and by members themselves. It was considered by the Review Group's Corporate Governance Committee.

1.1 Previous Report by the Company Law Review Group

The Review Group previously gave initial consideration to the issue of the obligation to disclose the residential addresses of an Officer in its *Report on certain Company Law Issues under the Companies Act 2014 relating to Corporate Governance* which was published May 2022. The relevant excerpt of that Report is set out in Appendix 1.

1.2 Context – Developments in Beneficial Ownership

The Central Register of Beneficial Ownership of Companies and Industrial and Provident Societies (**"RBO"**) was established to improve corporate trust and transparency in Ireland and the EU by making it clear to law enforcement agencies, regulatory authorities, designated persons, businesses and the general public who ultimately owns and controls Irish companies and industrial and provident societies.

The aim of the EU Directives that led to the establishment of the RBO is to deter money laundering and terrorist financing and to help law enforcement and regulatory authorities to identify those 'natural persons' who hide their ownership or control of Irish companies/societies for the purpose of facilitating illegal activities.

This Report by the Review Group is concerned specifically with the separate issue of disclosure of residential addresses of Company Officers. However, a judgement of the Court of Justice of the European Union in respect of the treatment of beneficial ownership in the Luxembourg Business Registers provides wider context.

On 22nd November 2022, the Court of Justice of EU ("**CJEU**") published it decision in *WM and Sovim SA v Luxembourg Business Registers.*[1] The case concerned the Fifth Anti Money Laundering Directive ("**5AMLD"**). In compliance with 5AMLD the Luxembourg Register of Beneficial Ownership had been designed in such a way that information on the beneficial ownership of registered entities could be retained and made available. Access to the data was publicly available. In certain exceptional circumstances, a beneficial owner could request the Luxembourg Business Registers ("**LBR**") to restrict access to specific authorities or entities.

[1] Joined Cases C-37/20 and C-601/20 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:62020CJ0037

A beneficial owner and a company challenged the decisions of the LBR denying their application to restrict the public's access to information concerning them. The referring Court considered that the disclosure of such information could entail a disproportionate risk of interference with the fundamental rights of beneficial owners.

The CJEU observed that since the data concerned included information on individuals, the access of any member of the general public to this data affects the fundamental right to respect of private life. In addition, making the information available required the processing of data. The CJEU found that making data available to the general public in such a manner was a serious interference with Articles 7 (Respect for private and family life) and Article 8 (Protection of personal data) of the Charter of Fundamental Rights.

Following the judgment, access to the RBO was suspended on 28th of November 2022 for designated persons and members of the public. Access was restored on 22nd of December 2022 to designated persons only. Access to the register by competent authorities was not affected. It is important to note that the residential addresses of beneficial owners were never available to members of the public, but only to competent authorities.

On 13th June 2023 the European Union (Anti-Money Laundering: Beneficial Ownership of Corporate Entities) (Amendment) Regulations 2023 was signed providing access to those who could demonstrate a legitimate interest (i.e. those engaged in the prevention, detection or investigation of money laundering or terrorist financing offences) but not to the general public. [2]

Criticism of the CJEU judgment was swift and to the point.[3] It ultimately led to the adoption of the 6th Anti-Money Laundering Directive (EU) 2024/1640 for the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Directive (EU) 2019/1937, and amending and repealing Directive (EU) 2015/849.

The 6th Anti-Money Laundering Directive, which must be transposed into national law by 10 July 2027, sets out the importance of identifying and verifying beneficial owners across entities. It also sets out how record retention and data protection clarifications would improve the work of competent authorities. It also aims to make sure that, rather than the general public, only those who could show a legitimate interest, such as journalists and civil society organisations could gain access to information on beneficial ownership in registers.

[2] S.I. No. 308/2023 - European Union (Anti - Money Laundering: Beneficial Ownership of Corporate Entities) (Amendment) Regulations 2023 https://www.irishstatutebook.ie/eli/2023/si/308/made/en/print
[3] See further: Paul Egan, 'Who are you?' Law Society Gazette, June 2023 at pp 38 to 43. lawsociety.ie/globalassets/documents/gazette/gazette-pdfs/gazette-2023/june-2023-gazette.pdf

2. Current Legislative Provisions

2.1 Summary of Current Legislative Provisions

The position in Ireland regarding the treatment of the residential addresses of Company Officers is neatly encapsulated in the Companies Act 2014 (the "**2014 Act**").

Pursuant to s 149 of the 2014 Act, a company shall keep a register of its Directors and secretaries, and, if any, its assistant and deputy secretaries ("**the Register**") ("**Relevant Officers**"). Subject to s 149(2)(c) of the 2014 Act, the Register shall contain the "usual residential address" of its Relevant Officers, amongst other particulars including date of birth, nationality and usual business occupation. Pursuant to s 216 of the 2014 Act, this Register must be available for inspection in person during business hours to any member of the company and to any other person for a fee, and a copy may be requested for a fee. There is an ongoing obligation on a Relevant Officer and the company concerned to update the Register and to notify the Companies Registration Office ("**CRO**") of any changes.

Failure to comply with this requirement is a category 3 offence under s 150(4) of the 2014 Act, punishable by a term of imprisonment of up to six months and a Class A fine of up to €5,000 (or both).

The usual residential address is filed, separately to the Register maintained by the company, with the CRO in various prescribed forms including:

- Upon company incorporation
- Upon changes in Director particulars or Director appointments/cessations, and
- Upon the submission of Annual Returns

The information is therefore subsequently publicly available information from the CRO and can be accessed by any member of the public upon payment of a fee.

The inclusion of the requirement for the usual residential address facilitates the identification of the Relevant Officer by both the CRO and more generally by the public (e.g. to distinguish Sam Smith with an address in Athlone and Sam Smith with an address in Bantry). It also facilitates direct communication with the Relevant Officers by the Registrar and others.

2.2 Members

In the case of Relevant Officers who are also members, pursuant to section 169(1)(a), a company shall also keep a register of members which includes their addresses. However, it is not specified that the address in question must be the usual residential address, and no other identifying personal particulars are required (for example date of birth). The policy intent of this section is to provide a means of contacting members for the operation of other sections of the Act rather than a means of identifying members. Members could provide an office address, business address or other address that is not their usual residential address should they elect to do so, and therefore this report does not give consideration to those provisions.

2.3 Identification of Directors by the CRO

Since 11 June 2023 and the commencement of the Companies (Corporate Enforcement Authority) Act 2021, it has been mandatory for a Director to provide their Personal Public Service Number **("PPSN**") when filing certain documents in the CRO. If a Director does not have a PPSN (generally because they are located outside of Ireland), the CRO will, on application, and subject to the provision of the required information, issue the applicant with an Identified Person Number ("**IPN**"). These numbers facilitate the identification by the CRO of the person who is a Director of a company. They support the verification of the Director as a real person and furthermore avoid duplication where there may be variations of a Director's name and address. It is to be noted that this provision does not apply to an individual who is appointed as a secretary, assistant or deputy. Such Officers are not required to provide their PPSN/IPN. The PPSN is not publicly available and the PPSN is not required on the Register kept by the company.

2.4 Exemption to Residential Address Requirement - Personal Safety and Security

Section 150(11) of the 2014 Act, provides that the Minister may make regulations providing an exemption to the requirements under s 149 of the 2014 Act. It provides that a Relevant Officer need not provide their residential address where:

> *… it is determined that the circumstances concerning the personal safety or security of the person warrant the application of the foregoing exemption in respect of him or her; and (b) such other conditions (if any) as are specified in the regulations for the application of the foregoing exemption are satisfied.*

Regulations were made pursuant to s 150(11) of the 2014 Act, namely the Companies Act 2014 (Section 150) (No. 2) Regulations 2015, S.I. No. 543/2015 (the "**2015 Regulations**"). In order to request an exemption of the residential address requirement:

a. The request for an exemption is sent to the Registrar in an envelope marked "For the Attention of the Registrar" and is accompanied by the forms specified for such purpose by the Registrar (T1);

b. The application requesting an exemption in accordance with section 150(11) of the 2014 Act is accompanied by a supporting statement from an Officer of An Garda Síochána not below the rank of a Chief Superintendent;

c. The statement contains a request that the usual residential address of a person who is an Officer of the company shall not appear on the Register kept by the Registrar for reasons of personal safety or security.[4]

Where the Registrar is fully satisfied that the Relevant Officer has fully completed the procedure in Regulation 3 of the 2015 Regulations, he or she shall notify the Relevant Officer that an exemption has been granted.[5] Where a residential address of the Relevant Officer is required, the registered office of the company shall be entered as opposed to his or her usual residential address.[6] A separate application is required requesting an exception in respect of each company that the Relevant Officer wishes to apply for an exemption.[7] Where the Relevant Officer is a shareholder of the company, the register of members shall be amended by the company by the removal of the Relevant Officer's residential address and the substitution therefor of the registered office of the company.[8]

Once an exemption has been granted by the Registrar, unless the residential address of the Relevant Officer is (inadvertently or otherwise) included in a document that is filed in the CRO, the Registrar has no record of the residential address of the Relevant Officer.

The CRO's website states that:

> *A T1 application is not retrospective and any document already registered with the CRO containing the residential address will not be redacted. The applicant is responsible for the non-disclosure of the residential address where the application is successful. The CRO accepts no responsibility for the subsequent disclosure of the address by the company on any form submitted to the CRO.*[9]

Approximately 2,000 such T1 applications have been received.

3. Presentations and Submissions Considered by the Review Group

On the 5th June 2025, the Review Group invited Dr Alexander Chance, Head of Policy and Research, from civil society organisation Transparency International Ireland and Mr David Murphy, Deputy Commissioner, Data Protection Commission to present to the Group on their perspectives relating to this topic. A summary of the presentations is outlined hereunder.

[4] Regulation 3, Companies Act 2014 (Section 150) (No. 2) Regulations 2015, S.I. No. 543/2015 https://www.irishstatutebook.ie/eli/2015/si/543/
[5] Regulation 4, Companies Act 2014 (Section 150) (No. 2) Regulations 2015, S.I. No. 543/2015
[6] Regulation 5, Companies Act 2014 (Section 150) (No. 2) Regulations 2015, S.I. No. 543/2015
[7] Regulation 6, Companies Act 2014 (Section 150) (No. 2) Regulations 2015, S.I. No. 543/2015
[8] Regulation 11, Companies Act 2014 (Section 150) (No. 2) Regulations 2015, S.I. No. 543/2015
[9] CRO website: https://cro.ie/post-registration/company-post/officer-address-disclosure/

The Review Group, in the course of its deliberations, considered a submission from the Law Society prepared in June 2024 as well the two presentations mentioned above.

3.1 Presentation by Transparency International Ireland

Dr Alexander Chance, Head of Policy and Research, from civil society organisation, Transparency International gave his presentation (set out in Appendix 2) and discussed the importance of functional transparency and the ability to access information in order to make informed decisions. Reliance is placed on transparency for the fight against criminal activity, in particular, money laundering. Dr Chance noted that the benefits of economic crime, at some point, end up in society. The question then to be addressed is what is reasonable in the context of privacy and the need to identify individuals.

Residential addresses are often publicly available online and in other sources; general locations are routinely found with ease using social media. Disclosure of usual residential addresses must be balanced against the security risk and a more general infringement of privacy including infringement of privacy of others who may reside in the home, such as partners, elderly persons, vulnerable persons or children.

The over publication of data beyond what is necessary could lead to a future risk of judicial over reaction. Some commentators would argue that this already has been the case with the CJEU decision in *WM and Sovim SA v Luxembourg Business Registers*. Therefore, any change must be capable of defence from legal challenge.

Dr Chance opined that the 2015 Regulations had significant shortcomings. A core criticism was the lack of procedures for the statement of support from the Chief Superintendent. A person must demonstrate a risk to his or her personal safety, which implies that a substantial threat has already materialised. Furthermore, there is no criteria to be considered by the Chief Superintendent, and discussion was had on the difficulties a Chief Superintendent could have in assessing a risk to a Relevant Officer not based in Ireland.

While larger and better resourced companies may have greater capacity to pursue such exemption for Relevant Officers, those in small and medium companies could also be considered to be at risk to their personal safety and security but less well-resourced to pursue such an exemption. Hypothetical examples given during the discussion were a small transport and logistics company whose Officers could be intimidated or put under pressure to engage in illegal activity by organised crime, or a small estate agent or accommodation provider who could be targeted by hate-motivated crime.

The Group discussed categories of companies that could be used to provide exemptions and although superficially attractive, such a system could be endless.

Additionally, improving the process to apply for the exemption, including recommendations to assist a Chief Superintendent (e.g. providing guidance and criteria) would not deal with the deficiency in the

2015 Regulations for a threat has likely materialised before an exemption is applied for, in which case the Relevant Officers residential address is already available on the Register.

Finally, Dr Chance highlighted the challenges with redacting historical information. This, he believed, undermined the exemption in the 2015 Regulations and how even inadvertently filing a residential address in the CRO would negate the exemption and thereby defeat the purpose of the 2015 Regulations.

In conclusion, Dr Chance, whilst supporting corporate transparency and the need to identify Relevant Officers, expressed support for the system such as that in the UK which protects the privacy of individuals but also provides continuous access to relevant information to particular categories of organisation and officials.

3.2 Presentation by the Data Protection Commission

The Data Protection Commission ("**DPC**") is the national independent authority responsible for upholding the fundamental right of individuals in the EU to have their personal data protected. The DPC is the Irish supervisory authority for the General Data Protection Regulation ("**GDPR**"), and also has functions and powers related to other important regulatory frameworks including the Irish ePrivacy Regulations (2011) and the EU Directive known as the Law Enforcement Directive.

A helpful presentation (set out in Appendix 3) was provided to the Group on the GDPR by officials from the DPC, who welcomed the opportunity to discuss potential legislative amendment in this forum although that office has no current view on the topic.

In the present circumstances, the data controller is the Minister for Enterprise, Tourism and Employment who has designated the Registrar of the Companies as the data processor. The lawfulness of data processing is contained in Article 6 of GDPR which includes that it must be necessary for compliance with a legal obligation and necessary for the performance of a task carried out in the public interest or in the exercise of official authority.

Therefore, the rights of the data subject (i.e. the Relevant Officer) need to be balanced with the legal obligations of the Data Controller (i.e. the CRO) and its public interest activities. Section 149(2) of the 2014 Act creates a legal obligation to process the residential address of an Officer. It predates the introduction of the GDPR. A legitimate question, therefore, is as to the necessity of this provision in order to be compliant with Article 6 GDPR. A related question is whether the legal obligation is proportionate to a legitimate aim.

The exemption in the 2015 Regulations may not safeguard the data subject rights as it places a responsibility on the Relevant Officer and is therefore not appropriate, particularly in circumstances where the Relevant Officer has already been targeted/identified and/or in conjunction with the inability to retrospectively redact the residential address already on public file.

An example was referred to in discussion of a public register of private ownership maintained by a commercial semi-state body responsible for certain aspects of regulation of a sector. This register previously contained the residential address of the owners. While no formal DPC action was taken, after consultation on the necessity and appropriateness of disclosing that information, it was amended. Current practice is now that only the county of residence of the owners who are individuals are published on the register published by the commercial semi-state body.

The DPC officials noted that data protection rights derive from EU law for which its office has responsibilities and that quite separately, privacy rights also drive from EU law but for which the DPC has no responsibilities.

3.3 Submission by the Law Society of Ireland

The Law Society made a submission to the Company Law Reform Group in June 2024. The submission focuses on Section 150 of the Companies Act 2014 and the Companies Act 2014 (Section 150) (No. 2) Regulations 2015 [S.I. No. 543 of 2015], particularly regarding the exemption process for Directors and company secretaries from disclosing their residential addresses on the public register. A summary of the submission is outlined in Appendix 4.

3.4 Approaches in Other Jurisdictions

In a number of other common law jurisdictions, for example Singapore, Directors must file a residential address, but have the option of supplying a Contact Address for the public register. [10] New Zealand previously had provisions that are similar to those currently in place in Ireland, but in August 2024, the government announced measures to suppress Directors' residential addresses from the Companies Register. [11] In other EU Member States, for example the Netherlands, a business may be incorporated using a residential address or a business address. A visiting address is also required, and there are provisions to shield this if it is also a residential address.[12]

The approach taken in the UK merits particular attention. As in Ireland, in the UK it has always been considered important that creditors, law enforcement and regulatory authorities should be able to identify and locate company Directors. A limited system of confidentiality was introduced in 2002, and with the introduction of the Companies Act 2006, a system of confidentiality was introduced for all Directors' residential addresses, which were regarded as protected information. Directors must supply a contact address and a usual residential address to Companies House, but the latter is not available on the public record. Regulations in 2009 permitted the Registrar to disclose information to specified public authorities and credit reference agencies, and provided a mechanism by which an individual can make an application to ensure their residential addresses are not provided to credit agencies where they consider that there is a serious risk of violence or intimidation.[13] Regulations in 2018 enable an individual whose usual residential address which is listed on the Directors' register (for example where

[10] Singapore Accounting and Corporate Regulatory Authority: https://www.acra.gov.sg/how-to-guides/before-you-start/addresses

[11] New Zealand Ministry of Business, Innovation and Employment, package of reforms of the Companies Act: mbie.govt.nz/business-and-employment/business/regulating-entities/companies-act-reforms

[12] Business Register (*Handelsregister*) of the Netherlands Chamber of Commerce KVK https://business.gov.nl/starting-your-business/registering-your-business/registration-at-the-netherlands-chamber-of-commerce-kvk/#art:what-is-recorded-in-the-business-register

[13] UK Companies (Disclosure of Address) Regulations 2009 https://www.legislation.gov.uk/uksi/2009/214/

it has been provided as a contact address) to apply to the Companies House to make the address unavailable for public inspection without having to demonstrate any requirement. [14]

4. Group Deliberations

The Group considered the current legislative provisions, the presentations from the invited presenters, the submission from the Law Society of Ireland, and the equivalent provisions in other jurisdictions including the UK.

The Group agreed in the first instance that the 2015 Regulations did not appear to be achieving their objectives. The Group gave due consideration to the concerns regarding the personal safety and security of Relevant Officers and that of those unconnected to the company but who may reside at the residential address such as partners, elderly persons, vulnerable persons and children. During deliberations, members of the Group gave examples where the public availability of a Director's residential address had caused personal safety concerns for an individual. It is also apparent that the public availability of this information may become out of step with international practice in some other jurisdictions.

4.1 Retrospective Applicability

The potential retrospective applicability and redaction of older filings held by the CRO was also considered. The CRO representative highlighted the costs involved with redacting all previous material, which would have to be moderated by an individual(s), would require considerable resources, involve potentially millions of documents and would incur significant cost and resources. Furthermore, bulk purchasers of CRO data (and their clients') already have that data which is publicly available on other websites and would still have the information thereby making it very challenging to ensure that the information which has already been disseminated by others is fully redacted.

It was suggested and accepted by the Group that a particular point in time be selected from which any change would apply. The norm for such change is that it is not retrospective and would apply when statutory changes come into effect.

5. Recommendations

1. The Group recommends legislative change to **preclude the default public availability without qualification, in the operation of the 2014 Act, of Relevant Officers' usual residential addresses as contained in the Register and submitted as prescribed to the CRO**. This recommendation is contingent on there being appropriate timely mechanisms for the CRO, members of the public, relevant authorities and other interested parties (such as creditors) to effectively engage with and identify Relevant Officers.

[14] UK Companies (Disclosure of Address) (Amendment) Regulations 2018 https://www.legislation.gov.uk/uksi/2018/528/

2. The Group recommends legislative change to require that, in addition to their residential address, **Relevant Officers provide a contact address**, which could be their usual residential address, the registered office of the company, or another address as prescribed. This contact address must be located in the State. The contact address will be the only address that appears to the public on the Register kept by the company and that is made publicly available without restriction by the CRO.

3. The Group recommends legislative change as above to also preclude the default public availability without qualification of residential addresses in the case of companies required to register pursuant to Part 21 of the 2014 Act (**external companies**).

4. The Group recommends that the legislative change proposed in the first recommendation **should provide for the timely permitted disclosure of the usual residential address**. The Group views that categories to whom disclosure is permitted should include competent authorities and other actors who require the usual residential address for the purposes of law enforcement, regulatory compliance and judicial proceedings. The Review Group recommends that the question of serving proceedings be clarified in the implementing legislation.

5. The Group recommends that, therefore, in a context where the usual residential address is no longer publicly available without restriction, the **2015 Regulations should be repealed** and **appropriate legislative change made to s150 of the 2014 Act**. Relevant Officers, who successfully made a T1 application and currently use the company's registered office address, should provide a usual residential address to the Registrar and failure to do so should be an offence.

6. The Group recommends that the legislative change does not have retrospective effect and applies from the date of the coming into effect of the statutory changes.

Appendices

Appendix 1

Extract Report on certain company law issues under the Companies Act 2014 relating to Corporate Governance, May 2022 (Disclosure of Directors Residential Address)

Issue 8 - Exemption from obligation to disclose home address of Directors (Sections 149 and 150(11))

Issue Section 149 of the 2014 Act requires that a company must deliver, within the period of 14 days after any change among its Directors or in its secretary or assistant or deputy secretary or any change in any of the particulars contained in the register, a notification of such event to the CRO. Accordingly, a Director's and secretary's residential address must be entered on a Form B10 (Notification of Change of Director or Secretary). In addition, it must be included on the Form B1 (Annual Return) and accordingly is publicly available on inspection of those documents when filed, and on derivative websites that make available such filed information.

Such an Officer's residential address can be omitted from those documents when filed, where the Officer's personal safety or security is at stake. This is to minimise potential risks to Officers of certain types of company (e.g., certain pharma or social network companies). The applicable law is S.I. No. 543/2015, the Companies Act 2014 (Section 150) (No. 2) Regulations 2015. Thus, any change would require that these regulations be changed.

The procedure to omit information on the forms involves obtaining a supporting statement from a person not below the rank of Chief Superintendent in An Garda Síochána and an application to the CRO. There are several shortcomings in the law and the procedure:
- addresses already on the CRO register cannot be redacted; - separate applications must be made for each company involved;

- the exemption is automatically cancelled where, even inadvertently, the Officer's home address is included on any CRO filing.
In addition, the new process is untested, and no guidance has been published as to the level of threat which must be involved, the evidence which must be produced or whether the Officer must appear in person at the police station. There seems to be no system in place within An Garda

Síochána to deal with applications of this type nor was there common knowledge of the provision among any of the stations contacted.
A submission of a practitioner considered by the Group proposed that:

(i) a dedicated unit or contact point within An Garda Síochána with the necessary resources be formally nominated (and/or details of same published) to deal with applications of this type;
(ii) guidelines be published as to the criteria to be used in granting any supporting statement by An Garda Síochána; and
(iii) procedures be put in place to allow Officers residing outside the State to make the relevant application through their Irish legal advisers.

Group deliberations

The Group concluded that the proposal had merit, particularly in an environment of increasing public scrutiny and a policy shift towards affording individuals a suitable level of privacy.
The Group noted the principle that there should be transparency of ownership and control of a company and noted the introduction of disclosure of beneficial ownership in Ireland. Historically, a key element of this was that there should be full details of a Director, including the Director's residential address. The CRO considered it would not be possible for an Officer's home address to be redacted retrospectively as the information would have been publicly available for a significant period and they would have no control over who had already accessed it.

However, the legislature saw fit to introduce an exemption to the disclosure of an Officer's residential address. In that regard, practical issues have arisen, particularly for non-resident individuals, and a review of the existing provisions in the context of a modern company law framework and environment is warranted.

CLRG Recommendation

The Review Group recommends that this issue be considered further by the Corporate Governance Committee as part of the future work programme for the Company Law Review Group, looking in particular at the desirability and practical issues arising with
- guidelines and criteria to apply to those who would seek to avoid disclosure of their residential address;

- the redaction of information already on the register; and

- the interaction of data protection law and the ethics of disclosure of Officer information under the Companies Act.

Appendix 2

Law Society Submission on Section 150 of the Companies Act 2014 and the Companies Act 2014 (Section 150) (No. 2) Regulations 2015

1. Introduction

1.1 The Law Society of Ireland (the "**Law Society**") wishes to make the following comments and recommendations on section 150 of the Companies Act 2014 (as amended) (the "**Act**").

1.2 This submission has been prepared for the Law Society by our Business Law Committee (the "**Committee**") which is comprised of practitioners with substantial experience and expertise in the law of public and private companies, insolvency law, partnership law, banking and financial services law, business regulation, foreign direct investment, competition law, the law of contract and consumer protection law. Additional input was provided by GDPR experts on the Intellectual Property & Data Protection Law Committee in the Law Society.

1.3 The Law Society previously made a submission to the Department of Jobs, Enterprise and Innovation in April 2016 which covered a number of proposals for amendments to the Act including section 150 (the "2016 Submission").

2 . Background and Summary

2.1 The purpose of this submission is to:

2.1.1 highlight a gap in the legislation that affects Officers (Directors and individual company secretaries) of entities registered under the Act ("**Affected Officers**") who are seeking an exemption from disclosing their residential addresses to the Companies Registration Office (the "**CRO**"),

2.1.2 request the Company Law Review Group ("**CLRG**") to progress the implementation of the recommendations for Issue 8 in the Company Law Review Group's Report on certain company law issues under the Companies Act 2014 relating to Corporate Governance dated May 2022 (and included in the CLRG's 2022 annual report) (the **"2022 report"**) with a view to recommending legislative changes to address the issues we have raised.

2.2 Section 150(11) of the Act and the implementing statutory instruments (SI 225/2015 and SI 543/2015) introduced a process allowing an Affected Officer's residential address to be omitted from the public register (and relevant company register) where the Affected Officer's personal safety or security is at stake. The policy objective behind

this measure was to minimise potential risks to Affected Officers of certain types of company where home address details were easily accessible to members of the public.

2.3 We are aware that the CLRG has also previously highlighted the shortcomings in the law and the procedure under Section 150(11) in its 2022 report, in particular that addresses already on the CRO register cannot be redacted under the current regime, separate applications must be made for each company involved; the exemption is automatically cancelled where, even inadvertently, the Officer's home address is included on any CRO filing and has recommended that these issue be considered further by the Corporate Governance Committee.

2.4 The 2016 Submission was also referenced in the Law Society submission to the Joint Committee on Enterprise, Trade and Employment on the General Scheme of the Companies (Corporate Enforcement Authority) Bill in December 2020 (the "2020 Submission").

2.5 The Law Society submits that the current procedure under Section 150(11) is of very limited use in practice. Notwithstanding some efficiencies which have been achieved, the exemption, once granted, only applies prospectively from the date the application is made, and an Affected Officer's personal address is not removed or redacted from any historic filings already on the public CRO register. Accordingly, the residential address of an Affected Officer can be easily obtained from a previous filing and the protection afforded by this process is effectively nullified. The Law Society recommends that procedures be put in place to exclude personal addresses from historic as well as future filings, as without this mechanic the protection is meaningless and only benefits incoming or newly appointed Affected Officers.

3. Issue

3.1 The default position under Section 149 of the Act is that particulars of an Affected Officer, including their residential address, must be disclosed to the CRO via submission of a Form B10, and are also required to be included in various other filings as well as the entity's annual return. As a consequence, the residential addresses of Affected Officers are publicly accessible on the Register of Companies (the "**Register"**) and such Affected Officers are under an ongoing obligation to notify the CRO of any change in their residential address and ensure the Register is updated accordingly. Failure to

comply with this requirement is a category 3 offence under the Act, punishable by a term of imprisonment of up to six months and a Class A fine of up to €5,000 (or both).

3.2 Section 150(11) of the Act contains an exemption from the general disclosure requirement, to permit Affected Officers to use the company's registered office address on the public record instead of their usual residential address (the "**Exemption**"), and provides:

> *The Minister may make regulations providing that any requirement of this Act that the usual residential address of an Officer of a company appear on the register referred to in section 149(1) or the register kept by the Registrar shall not apply in relation to a particular person who is such an Officer if -*
>
> *(a) in accordance with a procedure provided in the regulations for this purpose, it is determined that the circumstances concerning the personal safety or security of the person warrant the application of the foregoing exemption in respect of him or her; and*
>
> *(b) such other conditions (if any) as are specified in the regulations for the application of the foregoing exemption are satisfied.*

3.3 The regulations referenced in Section 150(11) are the Companies Act 2014 (Section 150) (No. 2) Regulations 2015 [S.I. No. 543 of 2015] (the "**2015 Regulations**") which set out the mechanic by which an Affected Officer may avail of the Exemption, as follows:

> *An application to request the exemption of the usual residential address of an Officer of a company from appearing on the register shall comply with the following:*
>
> *(i) The request for an exemption is sent to the Registrar in an envelope marked "For the Attention of the Registrar" and is accompanied by the form, if any, specified for such purpose by the Registrar;*
>
> *(ii) The application requesting an exemption in accordance with section 150(11) is accompanied by a supporting statement from an Officer of An Garda Síochána not below the rank of a Chief Superintendent;*
>
> *(iii) The statement contains a request that the usual residential address of a person who is an Officer of the company shall not appear on the register kept by the Registrar for reasons of personal safety or security.*

3.4 In practical terms, to avail of the Exemption, a Form T1 must be submitted to the CRO in respect of each company to which the Affected Officer has been or will be appointed, together with a supporting statement (the "**Statement**") from a Chief Superintendent of An Garda Síochána stating that the Exemption in respect of such Affected Officer is necessary on the grounds of personal safety or security. To obtain the Statement, the

Affected Officer must demonstrate that there is a risk to their personal safety or security, and the Law Society understands that An Garda Síochána can require examples of threats experienced by the Affected Officers to be included in the application for the Statement.

3.5 While the Exemption is helpful in theory, its application in practice is significantly constrained as the Exemption does not have retrospective effect, and the Affected Officer's residential address is not removed or redacted from any filings already on the public Register. The Exemption only operates prospectively with effect from the date the Form T1 is registered. As a consequence, the Affected Officer is only permitted to use the company's registered office address from the date of registration of the Form T1 and any filings made after that date, but their residential address is still visible and easily accessible by the public in any earlier filings which remain unchanged despite the Exemption. This means that where a Form T1 has been registered, for example in January 2024, the Affected Officer can use the registered office address in submissions made following that date, but their residential address can be easily obtained from the annual return filed in 2023 as well as any earlier filings in respect of that Affected Officer.

3.6 The CRO's position in not removing or redacting any residential addresses that are already disclosed on the Register is clearly indicated in the Form T1 as well as guidance published on the CRO website, as excerpted in Appendix 1 below. The Law Society also understands that the CRO has indicated that the Registrar of Companies (the "**Registrar"**) does not have the power, either express or implied, to remove any documents that are already registered on the Register and cannot take such action as they do not have the statutory power to do so. As such, any change in CRO procedure in this regard would require legislative amendment to provide this power to the Registrar and enable the CRO to remove references to residential addresses from historic filings.

3.7 We would also like to highlight the recent decision of the Court of Justice of the European Union ("**CJEU**") (joined cases C-37/20 and C-601/20) which restricted public access to a number of beneficial ownership registers, including the Central Register of Beneficial Ownership of Companies and Industrial and Provident Societies (the "**RBO**") operated by the CRO in Ireland. The CJEU found that permitting public access to registers of this nature (which include individuals' personal address details) constituted a breach of Articles 7 and 8 of the Charter of Fundamental Rights of the European Union and held that access to such information constituted a serious interference with the fundamental rights to respect for private life and the protection of personal data. As a consequence of this ruling, the CRO has limited access to the RBO to "designated persons" and competent authorities.

3.8 The Law Society also submits that the general publication of Directors' personal addresses raises potential issues under the EU General Data Protection Regulation (the "**GDPR**"). One of the key obligations under the GDPR is that any processing of personal data (which includes the collection and publication of personal data) must satisfy a condition for processing under Article 6 of the GDPR. It might be argued that Article 6(1)(c) (legal obligation) and Article 6(1)(e) (processing permitted by EU or Member State Law) provide such a legal basis in light of section 149 of the Companies Act (subject to the exemption under the 2015 Regulations). However, Article 6(3) of the GDPR provides that any EU or member state law which is relied on for the purposes of Articles 6(1)(c) or (e) must *"meet an objective of public interest and be proportionate to the legitimate aim pursued".* We think there is a material risk that section 149 (together with the limited protection afforded to a wide cohort of Affected Officers under the 2015 Regulations) does not meet this test. In addition, it is also open to question whether the publication of Directors' personal addresses without effective exemptions for Affected Officers meets the data minimisation requirements of Article 5(1)(c) of the GDPR which requires that any personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

3.9 Given the similarities between the details included on the RBO and the CRO, a similar argument can be made in favour of redacting Affected Officers' address details from filings already on the Register, on privacy as well as security grounds. Accordingly, the Law Society recommends that a change to current practice is introduced and seeks the support of the CLRG in proposing an amendment to the legislation in this regard.

4. Recommendations and Conclusion

4.1 The Law Society submits that the Exemption affords very little protection to Affected Officers where details already on the Register remain unchanged and are easily accessible, and the policy objective underpinning the arrangements under section 150 and the 2015 Regulations is not being appropriately addressed and achieved.

4.2 The Law Society reiterates its recommendations set out in the 2016 Submission that:

4.2.1 a dedicated unit or contact point within An Garda Síochána with the necessary resources be formally nominated (and/or details of same published) to deal with applications of this type;

4.2.2 guidelines be published as to the criteria to be used in granting any supporting statement by An Garda Siochána; and

4.2.3 procedures be put in place to allow Directors residing outside the State to make the relevant application through their Irish legal advisers.

4.3 We are aware that the CLRG has also previously highlighted the shortcomings in the law and the procedure under Section 150(11) in its 2022 report, in particular that addresses already on the CRO register cannot be redacted under the current regime, separate applications must be made for each company involved; the exemption is automatically cancelled where, even inadvertently, the Officer's home address is included on any CRO filing and has recommended that these issues be considered further by the Corporate Governance Committee.

4.4 The Law Society echoes the recommendations of the CLRG and reiterates our earlier submissions on this procedure. The current Irish laws were formulated in a pre-internet era, and their continued application now fundamentally ignores the ease and speed at which information can be accessed online and individual safety and rights to privacy. Where an Affected Officer has already demonstrated to An Garda Siochána that there is risk to their personal safety or security (and has obtained a statement to that effect), the policy objective of affording protection to such individuals fails entirely unless residential addresses are removed from all public filings or the Exemption is inadvertently lost. It therefore follows that for the Exemption to have any meaningful effect, an amendment to the legislation and existing procedures to enable filings to be redacted and Exemptions to be maintained is necessary and important.

4.5 Our attention has been brought to the experience of Affected Officers of certain classes of company, for example, in the technology and related sectors and high-profile multinationals, who have received serious threats and been the subject of a number of public order incidents including intrusion of their personal homes. The continuing disclosure of the residential address of those individuals poses a significant risk to their public safety and represents a considerable disadvantage of accepting an Irish Directorship for those who have legitimate concerns. This seems particularly unfair where Affected Officers have already demonstrated the risk to their safety via the established Garda process.

4.6 The current system with its significant limitations on the Exemption makes Ireland an unattractive location for Directors of certain companies.

4.6 The Law Society recommends that the Form T1 should be amended to permit one application for all companies that an Affected Officer is appointed to. The practice of having to make separate applications for each company involved is disproportionate, inefficient and an unnecessary use of resources in an era of sustainability and developing technologies.

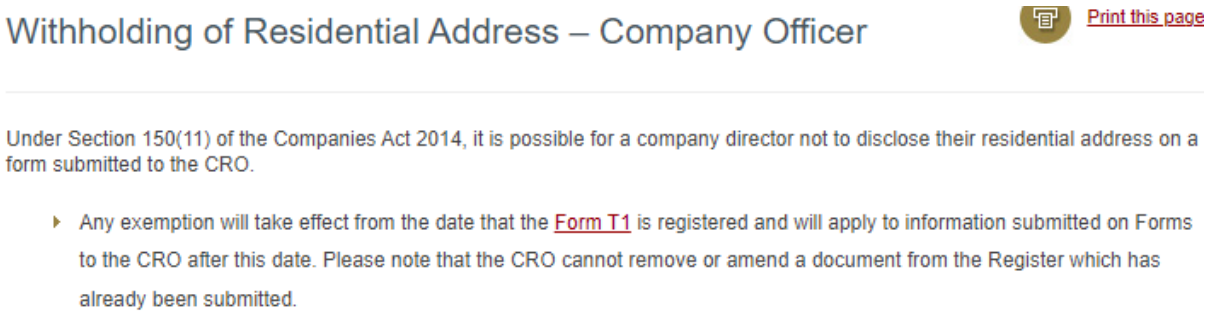
4.7 The Society recommends that the process that the Exemption is automatically cancelled where, even inadvertently, the Affected Officer's home address is included on any CRO filing should cease. With the advances in technology and the move to online filings via CORE a system should be put in place to prevent such filings being accepted by the CRO and instead such submissions should be rejected and not uploaded by the CRO.

4.8 For Affected Officers that are not resident in Ireland the Law Society recommends that procedures be put in place to allow applications to be made through their Irish legal advisers.

4.9 We hope that the CLRG will find the above comments constructive and helpful. The Law Society will be happy to engage further with the CLRG if required.

Appendix 1

CRO Website



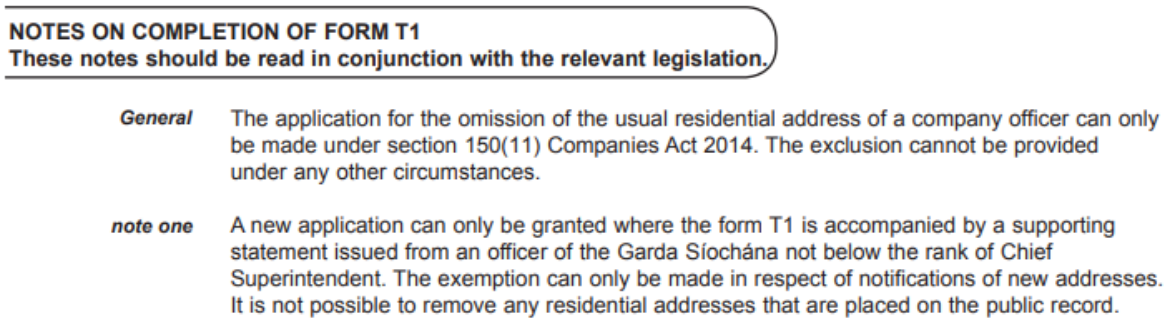
Withholding of Residential Address – Company Officer

Print this page

Under Section 150(11) of the Companies Act 2014, it is possible for a company director not to disclose their residential address on a form submitted to the CRO.

- Any exemption will take effect from the date that the Form T1 is registered and will apply to information submitted on Forms to the CRO after this date. Please note that the CRO cannot remove or amend a document from the Register which has already been submitted.

Form T1



NOTES ON COMPLETION OF FORM T1
These notes should be read in conjunction with the relevant legislation.

General The application for the omission of the usual residential address of a company officer can only be made under section 150(11) Companies Act 2014. The exclusion cannot be provided under any other circumstances.

note one A new application can only be granted where the form T1 is accompanied by a supporting statement issued from an officer of the Garda Síochána not below the rank of Chief Superintendent. The exemption can only be made in respect of notifications of new addresses. It is not possible to remove any residential addresses that are placed on the public record.

For further information please contact:

PolicyTeam@lawsociety.ie

Law Society of Ireland, 2024

Blackhall Place, Dublin 7
t. 01 672 4800
e. general@lawsociety.ie

Appendix 3

Transparency International Ireland Presentation

REVIEW OF THE PROVISIONS AND PROCESS PERTAINING TO DISCLOSURE OF DIRECTORS' RESIDENTIAL ADDRESSES, HAVING REGARD TO TRANSPARENCY REQUIREMENTS AND GDPR

Presentation by Dr Alexander Chance, Transparency International (TI) Ireland,
to the Company Law Review Group (CLRG) Corporate Governance Sub-Committee

Dublin, 5 June 2025

1. Introduction and background

Thank you for the kind invitation to address the sub-committee; it's a pleasure to be here this morning. Before getting to the issue at hand, it may be worth briefly providing some background on my professional experience and outlining how it has influenced my approach to transparency. It also allows me to give the important caveat that I'm not a specialist in company law. I've spent most of the past 20 years working on transnational organised crime and corruption; first within UK law enforcement and in more recent years from within civil society, focussing on the policy context that either constrains or facilitates serious criminality. So, perhaps unusually for a transparency advocate, I understand not only how access to information is critical to detecting and investigating crime, but also how personal data can be used and abused by criminals – which I'll come back to shortly.

Here I might also say a couple of words about Transparency International, or 'TI' as we're known, for those of you who aren't familiar with us. TI is a global movement dedicated to fighting corruption with national chapters in over 100 countries – including some that operate in exile – and a global secretariat in Berlin. If you've heard of TI before, it's most likely due to our annual Corruption Perceptions Index, which ranks every country. But TI does a lot more across casework, legislation, policy, research, advocacy and so on. At TI Ireland, we have five main areas of work, focussing on:

(i) Political integrity and ethics in public office;
(ii) Illicit finance (which is most relevant to our discussion today);
(iii) Institutional transparency and accountability;
(iv) Integrity in the workplace; and
(v) Supporting whistleblowers.

We also have a sister organisation, the Transparency Legal Advice Centre, which is staffed by solicitors who specialise in providing legal advice on protected disclosures. Although we're a small organisation, our close collaboration with colleagues in other countries gives us a global reach – in particular at the European level. For example, our current work on cross-border corruption and money laundering is carried out in conjunction with TI colleagues in eight other EU countries and with TI's office which works with the EU institutions. In general, we advocate for what one might call 'functional transparency', whereby people have access to the information they need to make informed decisions. That can mean voters having access to information on political candidates' declarations of interests, in order to ascertain if those interests have influenced their voting record, for example. In another context, it could mean comprehensive information being published on the awarding of public procurement contracts, so that businesses can be sure of a level playing field.

Today, rather than mount a strident defence of the status quo, I'm going to walk through a few questions that, I hope, will add a different perspective to your deliberations around the disclosure of Directors' residential addresses. First, I am going to take a step back to look at the wider context for this discussion, focusing on the role of company transparency and changing expectations of privacy. I am then going to explore some key considerations if the section 150 (11) procedure is maintained in some form, before concluding by examining the public disclosure requirement itself.

2. The wider context of corporate transparency

Whilst I'm cognisant that there are many other compelling reasons for creating and maintaining a transparent business environment, it's perhaps worth beginning our discussion by reemphasising the specific and critical importance of company transparency to the fight against modern-day economic crime. Here I need to dispel any notion that the criminal 'underworld' exists in an entirely separate or parallel universe to that of legitimate business. The reality is that *il*licit activities are dependent on the very same structures and processes as those used by licit businesses – so much so that Europol devoted a whole section of its most recent Serious and Organised Crime Threat Assessment to the criminal use of legal business structures. Use of such structures is of course particularly relevant to (but by no means limited to) money laundering itself, which is sometimes described as the 'lifeblood' of serious and organised crime. Irrespective of the illicit commodity or service that criminals deal in – whether drugs, guns, stolen personal data, or even human beings – at some point they have to get the proceeds of their activities into the legitimate economy if they are to enjoy their ill-gotten gains, or to reinvest it into future criminal ventures. And this is true not only for 'conventional' organised crime, but also for other illicit activities, such as corruption, tax evasion or sanctions evasion. Even politically or ideologically motivated illegal activities, such as terrorism – which don't have a profit motive – still require funding for their activities, and for that funding to be hidden from authorities.

In all these cases, the more opaque and secretive the business structure in question, the better for bad actors of various stripes. This is why the move towards beneficial ownership transparency has been such a critical move forward in the fight against money laundering and other illicit activities, why the *quality* and *reliability* of asset, company and beneficial ownership information really matters, and why *access* to that information is so vital, not only for our own domestic law enforcement agencies and regulators, but also for foreign authorities, journalists, civil society organisations and – we would argue – for normal citizens, all of whom can and do have a role in exposing a wide range of wrongdoing beyond just money laundering or terrorist financing. Indeed, as Paul Egan SC has eloquently argued in various publications, corporate transparency – including but not limited to beneficial ownership information – has far wider utility and application than merely the prevention and detection of crime. It is based upon a long-established social contract or social bargain that the privilege of limited liability comes with a corresponding duty of disclosure about who benefits from that privilege. And while we don't have time today to go into those wider societal benefits, a couple of quick examples might include knowing who owns and controls influential media platforms, or who sits behind companies responsible for environmental damage.

But, of course, transparency must be balanced against other considerations – in particular the right to privacy, which I'm sure the DPC will elaborate on shortly in terms of the role of data protection in safeguarding that right. In seeking to contextualise our discussion, it's worth highlighting that expectations of privacy have changed – and are changing – quite markedly in recent years due to social, economic and technological developments. We may be ever more aware of data protection rights and obligations, in particular in relation to how companies or state entities use our personal information, but many of us are simultaneously quite willing to publish highly personal information online to an unlimited global audience. This is relevant to our discussion around the disclosure of Directors' residential addresses because our home locations are sometimes openly available online or identifiable, with minimal effort, from open source research – which raises questions around both

consistent approaches to this issue across different state-run (and corporate) datasets, as well as how these trends influence our perception of reasonable expectations of privacy. To illustrate this, a quick review of publicly available datasets shows that I might be able to identify your exact home address or at least proximate location from the following sources, particularly if I already know your county, town/city or local authority area: (i) planning applications; (ii) electoral registers (the Seanad electoral register seems to have no opt-out facility); (iii) the Land Registry; (iv) local newspaper or community webpages; and, of course, (v) social media profiles, which can be a veritable treasure trove of personal information. (Indeed, it is no secret that law enforcement agencies, intelligence services and criminals themselves now routinely use social media for surveillance purposes, since social media posts can in many cases reveal a person's habitual home, work or leisure locations.)

Notwithstanding this increasing availability, however, it remains the case that one's residential address is a particularly sensitive piece of personal data. For those with a credible threat against their personal safety or security, revelation of their home address extends the threat to partners, family members and neighbours, quite possibly including children and vulnerable or elderly adults. The public disclosure of a residential address *must* therefore be weighed against the policy objective of that disclosure, which appears to be ensuring the transparent and unambiguous identification of company Officers. This identification factor is also vital and worth discussion. There *is* merit in a system that mitigates against the risk of inadvertent misidentification – a risk that is exacerbated where, for example, a Director has a common name and lives in a densely populated area – however that risk again has to be balanced against both the security risk posed to some Directors and the more general infringement of privacy posed to all residents of a particular residence by the publication of that address. (I will come back to this shortly – and I'm sure that our colleague from the DPC will have plenty more to say about the specific data protection issues on this point.)

There is another broader issue here that's worth highlighting, which is the argument that by publishing the residential addresses of all Company Officers, the current approach places the wider corporate transparency framework at risk of future judicial 'overcorrection'. We saw some evidence of this in the CJEU's judgment in the joined W.M./Sovim case, whereby the Court's taking issue with the public disclosure of beneficial ownership information resulted in the rolling back of public access to beneficial ownership registers – a retrograde step, in our opinion, that in Ireland's case is yet to be properly rectified, and may not be until the transposition of the sixth AML Directive. The detail of the beneficial ownership transparency debate is perhaps for discussion another time, but suffice to say that the CJEU's 2022 ruling was motivated, in part at least, by the Court's concerns that the fifth AML Directive overreached in terms of publication of personal data – or, to be precise, that it created the *potential* for publication of further personal data. In a domestic context too, we have arguably seen some indications of similar concerns coming through in various restrictions on what were previously publicly available data points, albeit on a smaller scale – including, for instance, in the DPC's approach to the disclosure of private aircraft owners' residential addresses on the publicly available Irish Aircraft Register. As an advocate for transparency, I want to see judicious approaches to the use of personal data, which can be robustly defended against legal or regulatory challenge, and which don't thereby expose the wider corporate transparency framework to the danger of Sovim-type judicial over-reactions, or over-corrections. Some of my colleagues might disagree, but I think on this point that the public disclosure of residential addresses presents not insignificant dangers.

3. Considerations for improving the s.150 (11) regime

Moving on to considering possible improvements to the section 150 (11) regime, I'm going to take as my starting assumption a level of dissatisfaction with the current procedure. That much is clear from your own annual report of 2022, from the Law Society's 2024 submission on the issue, and from the helpful memorandum drawn up by Katie Nagle BL – all of which were circulated before this meeting. Given that the general consensus across these documents is that the current approach has significant shortcomings, it's incumbent upon us to ask if, and how, the current system – as laid out in section 150 (11) of the 2014 Act and Statutory Instrument No. 543 of 2015 – can be improved.

One core criticism outlined in the aforementioned papers is the lack of an established procedure to assist a Chief Superintendent in deciding whether or not to support a section 150 (11) application. It is understood that, in order to obtain a Chief Superintendent's statement of support, the Company Officer must demonstrate that there is a risk to their personal safety or security – a risk that, according to the Law Society's submission, may require the provision of examples of the threats experienced. This poses several issues. First, it implies that a substantive threat must already have been made or even acted upon, in which case the exemption provision loses much of its utility as a protective mechanism; akin, perhaps, to waiting for a serious road traffic accident before making changes to a road junction that is patently dangerous. Moreover, in cases where a targeted threat has already materialised, it is not unreasonable to assume that the aggressor already has a degree of knowledge about their intended victim – including, perhaps – their home address. Of course, in some cases an applicant will be able to demonstrate a threat that has yet to be carried out – for example, online threats that have yet to be realised in the real, physical realm. However, notwithstanding such cases, if section 150 (11) is intended to *protect* personal safety and security, it is arguable that the exemption procedure cannot rely solely on an already demonstrated threat.

A related deficiency is the charge that the current procedure provides little or no consistency in terms of the criteria that must be met for a Chief Superintendent to provide their statement of support. Whilst senior gardaí are used to making informed and reasoned judgments – including, for instance, on threats to life in the context of organised crime and terrorism cases – the apparent absence of guidance for less clear-cut scenarios is unfair not only for applicants and but also for Chief Superintendents assessing their applications. What constitutes, to use the Act's current wording, 'circumstances concerning the personal safety or security' of the applicant that 'warrant … the exemption'? It is a vague and subjective standard. As we have explored, waiting for a demonstrable threat is problematic in itself. But what is the threshold to be used for gauging that threat in a consistent manner, and where might a line be drawn? There are, after all, innumerable possible threats to Directors' safety and security. The Law Society draws attention to 'certain classes of company, for example, in the technology and related sectors and high-profile multinationals', who have received serious threats and been the subject of a number of public order incidents, including intrusion of their homes. Whilst I would in no way diminish the seriousness of those incidents, I would suggest that many (if not most) security threats to Company Officers reach far beyond the tech sector or large multinational corporations, to small or medium sized firms that rarely have the benefit of corporate security teams, sophisticated equipment, training or other such measures.

Drawing on real-life examples, I can think, for instance, of the Directors of a small haulage firm, or a mid-size company that provides services in a port, or a wholesale florist who imports from the Continent. Such entities can be the subject of serious threats from trafficking groups; threats that are often implied rather than explicit, threats that typically come with demands for certain acts or omissions on the part of the recipient, and threats which don't lend themselves to being neatly recorded for passing on to a senior Police Officer. Looking to other types of threats, including those that may be ideologically motivated, do we cover certain demographic categories of Director, for example those belonging to religious minorities who have suffered abuse or threats, or to former guards who were involved in sensitive investigations into paramilitary groups? Or to Directors of pharmaceutical firms whose subsidiaries have carried out animal testing? Or to the owners of local hotels that accommodate international protection applicants? Or to the trustees of charities – also registered as companies – that provide services to asylum seekers? My point here is that seeking to provide exemptions to certain classes of company, or to certain categories of individuals, once again begins to raise questions around the criteria used to assess threat, the extent to which applicants are able to demonstrate that threat, and – ultimately – to the *consistency* of the protection afforded by section 150 (11). And if we choose *not* to use classes of company or demographic categories, we arguably come back to the deficiencies of a system in which applicants must demonstrate a threat.

On more practical points, the current situation whereby the Companies Registration Office is unable to retrospectively apply the exemption is discussed extensively in the documents we have before us, as is the process whereby the exemption is automatically cancelled if a home address is inadvertently included on any CRO filing. I won't re-hash the arguments already made on these points beyond stating my agreement with the Law Society that both issues serve to undermine the practical utility of the section 150 (11) provision. If, therefore, the decision is made to continue with an improved version of the current approach, I would agree that legislation and procedures should be amended to apply the exemption retrospectively across publicly available CRO datasets, and that the practice of automatically cancelling exemptions after any inadvertent filing of a home address should be discontinued. For the exemption to mean anything, it must be robust and effective.

There are a couple of other practical considerations if the exemption procedure is to be maintained. The first concerns Chief Superintendents' ability to properly assess exemption applications in the context of serious ongoing concerns over their existing workload, not least as a result of increased responsibilities under the current Garda Operating Model. This, in turn, is likely to affect the ability of those seeking an exemption to have their applications processed within the statutory timeframe for registering the appointment of a new Company Officer. It also raises the question of the extent to which a pressed Chief Superintendent is able to carry out reasonable enquiries to assess the validity of an application under section 150 (11) – particularly if that necessitates enquiries overseas to ascertain the nature and seriousness of an alleged threat. Given current demographic changes and trends in Ireland, such applications are likely to be increasingly common, yet international enquiries are typically time-consuming and, for non-emergency or non-priority requests, can take a very long time to elicit a response – if indeed they receive any response at all. Moreover, for those exemption applications that have an international dimension – including from company Directors who are themselves based overseas – one has to bear in mind that perceptions and thresholds of threat can vary quite significantly between policing authorities in different parts of the world.

4. Concluding thoughts: towards removal of public disclosure?

I've outlined the necessity for corporate transparency in terms of tackling economic crime and other illicit activities, and I've explored some of the considerations that need to be borne in mind if the exemption process is left in place. Taking all this into account, what tentative conclusions can we draw? In terms of the contribution of disclosure of a residential address to corporate transparency, I think one has to draw a distinction between being able to positively *identify* a Company Officer, and the ability to *locate* that individual's home address. Whilst I believe that the ability of any citizen to identify a Company Officer is an important public good – and a crucial part of the social contract that Directors enjoy in return for limited liability – it does seem legitimate to question whether the ability of any person to *locate* that individual's private residence constitutes an essential or integral aspect of corporate transparency. It is of course imperative that relevant agencies of the State – such as gardaí, the Corporate Enforcement Authority or relevant regulatory bodies – retain the ability to
locate a Company Officer's private residence, but there undoubtedly remain not insignificant issues with the *general publication* of this personal information. As we've explored, the current procedures for granting exemptions to publication have several deficiencies, and efforts to improve those procedures are unlikely to be able to address all of those issues, raising questions around their fairness and consistency, as well as facing not insignificant practical barriers and obstacles. I remain concerned that, if these deficiencies are not properly addressed, there remains a risk of future judicial or political overcorrection that places further limits on access to critical corporate data.

For this reason, I think that it is worth considering models that omit the requirement to publicly disclose residential addresses whilst ensuring that these details are available to those who need it in order to discharge their statutory duties or obligations. In this respect, the regime established in the UK would appear to have some merit. As Katie Nagle's memorandum explains, this approach: protects privacy whilst allowing continued access to residential addresses for those bodies that need it; makes provision for retrospective removal of home addresses, if required; and maintains an exemption system for withholding wider information in exceptional circumstances, for which there is a clear and high threshold – which a significant proportion of applicants reportedly fail to meet.

Most importantly, though, these measures have in recent years been complemented by a wholesale reform of the UK's approach to company registration and beneficial ownership transparency, most notably via the Economic Crime and Corporate Transparency Act 2023, or 'ECCTA'. Whilst the new arrangements are far from perfect, reform of these crucial areas was well overdue in the UK, and we would do well consider similar reform in our own context here too. Amongst its various provisions, ECCTA enhanced the transparency and accountability of limited partnerships, bolstered beneficial ownership reporting requirements around nominees and trustees, strengthened identity verification and – crucially – increased the powers, duties and resources of Companies House to verify information submitted to the register, and to carry out investigations and take

enforcement action. All of which are steps that we have long argued as being necessary in Ireland in order to build a more transparent and reliable business environment, and to effectively tackle economic crime.

It's within that context that I make my comments this morning; reform of section 150 (11) may indeed be necessary, but our framework for corporate transparency needs much wider attention. Thank you for your attention. I look forward to taking any questions during our discussion.

Appendix 4

Data Protection Commission Presentation

5th June 2025

Contents

An Coimisiún um Chosaint Sonraí
Data Protection Commission

An Coimisiún um Chosaint Sonraí
Data Protection Commission

Data Protection Commission
- **Independent supervisory body for the General Data Protection Regulations (GDPR)**

Public Sector Consultation and Supervision Team
- **Guidance and advice to public sector bodies in the pursuit of compliance with data protection laws**

@DPCIreland

Data Protection Commission Ireland

www.DataProtection.ie

Data Protection Legislative Framework

- General Data Protection Regulation (GDPR)
- The Law Enforcement Directive (Directive 2016/680)
- Data Protection Act 2018
- ePrivacy Regulations (SI 336/2011)

Key Definitions

Key Definitions – "Personal Data" and "Data Subject"

Article 4(1) GDPR

- **Any information relating to an identifiable natural person**
- **Identifiable natural person = data subject**
- **Identifiable by reference to:**
  - **Name**
  - **ID number**
  - **Location data**
  - **Online identifier**
  - **Factors specific to the physical, physiological, genetic, mental, economic, culture or social identity of the natural person**

An Coimisiún um Chosaint Sonraí
Data Protection Commission

Key Definitions – "Processing"

Article 4(2) GDPR

- **Any operation or set of operations performed on personal data such as:**
  - **Collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available**
- **Applicable regardless if the process is automated**

An Coimisiún um Chosaint Sonraí
Data Protection Commission

Key Definitions – "Data Controller"

Article 4(7) GDPR – defines controller

- **Natural or legal person, public authority, agency or other body who determines the purposes and means of processing personal data**
- **Minister for Enterprise, Tourism and Employment = data controller**

An Coimisiún um Chosaint Sonraí
Data Protection Commission

Key Definitions – "Data Processor"

Article 4(8) GDPR – defines processor

- **Natural or legal person, public authority, agency or other body who processes personal data on behalf of the controller**
- **Section 887(2) Companies Act 2014 – delegates Registrar of the CRO as the data processor for the Minister for Enterprise, Tourism and Employment**

An Coimisiún um Chosaint Sonraí
Data Protection Commission

Lawfulness of Data Processing (Article 6)

a) Consent of the Data Subject
b) Necessary for the performance of a contract
c) Necessary for compliance with a legal obligation
d) Necessary to protect the vital interests of the data subject or another person
e) Necessary for the performance of a task carried out in the public interest or in the exercise of official authority
f) Necessary for the purposes of the legitimate interests of the data controller

An Coimisiún um Chosaint Sonraí
Data Protection Commission

Data Processing by Public Bodies

Legal Obligation - Article 6(1)(c)
- Principle of necessity applies
- Based clearly on EU or MS law
- Clarity, precision, and foreseeability
- No discretion on the part of the controller

Public Interest – Article 6(1)(e)
- Based on EU or MS law
- Processing is necessary to achieve a purpose or task set out in law
- Wider discretion but **necessity and proportionality** apply

An Coimisiún um Chosaint Sonraí
Data Protection Commission

Article 6(3) GDPR

- Lawful processing under Art. 6(1)(c) and (e) must be laid down in EU law or Member State law
- Legal basis may contain further provisions defining the conditions of processing, e.g. the type of data collected, processing operations etc
- Such further provisions must include measures to ensure lawful and fair processing
- Must meet an objective or public interest and be proportionate to a legitimate aim

An Coimisiún um Chosaint Sonraí
Data Protection Commission

Recital 41 GDPR

- Legislative Act adopted by the Oireachtas is not a strict requirement, provided it is not contrary to the Constitution, to form a legal basis or legal measure
- Legal bases/measures ought to be clear, precise and be foreseeable in their application to affected persons
- Must be in accordance with CJEU and ECtHR jurisprudence

An Coimisiún um Chosaint Sonraí
Data Protection Commission

Rights of the Data Subject

- Right to information (Articles 12-14)
- Right of Access (Article 15)
- Right to Rectification (Article 16)
- Right to Erasure (Article 17)
- Right to Restrict Processing (Article 18)

An Coimisiún um Chosaint Sonraí
Data Protection Commission

Balancing Rights with the Public Interest

- Legitimate expectations and Rights of the Data Subject need to be balanced with public interest activities and legal obligations of the Data Controller
- Section 149(2) Companies Act 2014 creates a legal obligation to process residential address of company officers
- What is the necessity of this provision in order to be compliant with Article 6(1)(e) GDPR? Is it proportionate to a legitimate aim?

An Coimisiún um Chosaint Sonraí
Data Protection Commission

Safeguarding Data Subject Rights

- Section 150(11) Companies Act 2014 – empowers the Minister to make regulations exempting the provision of a residential address
- S.I. No. 225/2015 Companies Act 2014 (Section 150) Regulations 2015
  - Regulation 3 provides the procedure for applying for an exemption
  - Once this procedure is followed, granting an exemption is mandatory
  - However, it does not act retrospectively
- Is this a sufficient safeguard of the Data Subjects rights?

An Coimisiún um Chosaint Sonraí
Data Protection Commission


An Coimisiún um Chosaint Sonraí
Data Protection Commission
Thank you, any questions?
@DPCIreland
Data Protection Commission Ireland
www.DataProtection.ie