An Roinn Fiontar,
Turasóireachta agus Fostaíochta
Department of Enterprise,
Tourism and Employment

Public Consultation on proposed changes to the Companies Act 2014 and related legislation

Response Template

As set out in the Public Consultation paper, the Department of Enterprise, Tourism and Employment is seeking the views of stakeholders and interested parties on proposed changes to the Companies Act 2014 ("the 2014 Act'), in relation to access to the residential addresses of company officers and with similar changes to be reflected in the drafting of the Co-Operative Societies Bill and the Registration of Limited Partnership and Business Names Bill.

Please include your response in the space underneath each question and set out/ explain your views. Completing the template will assist with achieving a consistent approach in responses returned and facilitate collation of responses.

Respondents have the opportunity to comment more generally in the questions at the end of each section should they wish.

When responding please indicate whether you are providing views as an individual or representing the views of an organisation.

Name(s):	[redacted]
Organisation:	Lionheart Corporate Governance
Email address:	[redacted]@lionheart.ie
Telephone number:	[redacted]

Respondents are requested to return their completed templates by email to companylawconsultation@enterprise.gov.ie by **5pm on Friday, 19th December 2025.**

Section A: Proposed amendments to the Companies Act 2014

Implications of the proposed changes for information maintained by companies:

Question A1: **Do you have any views on the intended approach relating to the maintenance by companies of address details of relevant officers?**
Response: Yes. Lionheart supports the proposed approach: • We agree that the publicly available "Register of Directors and Secretaries" should contain only a "contact address" (which may be company-registered office or another suitable address), rather than the residential address by default. This mitigates privacy and security risks for directors and their families. • At the same time, the company should continue to record the "usual residential address" internally (and file it with the CRO) to enable lawful service, legal process, regulatory oversight and compliance. • This dual-layer system strikes the right balance: it preserves transparency and accountability where needed, without exposing sensitive personal data indiscriminately.

Implications of the proposed changes for filing with the Companies Registration Office:

Question A2: **Do you have any views on the intended approach relating to the filing with, and maintenance by, the Companies Registration Office of address details of relevant officers?**
Response: We endorse the proposal that: • The CRO continues to receive "usual residential addresses" even if they are not publicly disclosed. This ensures the register remains complete and accurate, and that mechanisms for service of documents, regulatory oversight, and legal process remain intact. • The publicly accessible CRO register should show only the "contact address" for each relevant officer. Public access to private residential data should be restricted to a defined set of legitimate users/entities (e.g. regulators, enforcement agencies, courts). • The system should be underpinned by robust governance of access: only clearly defined entities should have access, subject to appropriate safeguards.

Restricted access to the "usual residential address":

Question A3: **Do you have any views on the proposed list of entities that may be granted access to the "usual residential address" of relevant officers?**
Response: Lionheart believes the proposed list is broadly appropriate. We particularly support access by regulatory, law-enforcement and judicial authorities (e.g., police, financial-intelligence units, courts, relevant regulatory bodies). This is consistent with legitimate public-interest, regulatory and enforcement needs. However, to ensure proportionality and minimise privacy risk, we recommend that: • Access mechanisms should include clear evidentiary thresholds and a requirement to show "legitimate interest" before approving requests. • There should be audit-logging of access requests and a process for data-subject notification, where appropriate, subject to confidentiality and legitimate enforcement needs. • The legislation should expressly forbid public (open) redistribution of residential address data, or its use for non-official/political purposes (e.g. vigilante enforcement, harassment).

Question A4:

Are there any other comments you wish to make on the proposed approach to dealing with the "usual residential address" of relevant officers?

Response: Yes. In addition to the above:

- We suggest that the reform clarify in legislation the purposes for which the private residential address may be used — e.g., service of process, enforcement, regulatory compliance — and prohibit non-essential uses (marketing, unsolicited contact, profiling, data mining, etc.).
- Given the sensitivity of residential address data, we recommend introducing data-protection safeguards within the statutory scheme, e.g. requirement for secure handling, storage, limited access, retention only for as long as needed, and periodic review of necessity, in alignment with GDPR principles (data minimisation, purpose limitation, security).
- We support the proposal that previous filings (i.e. existing public residential addresses) remain for historical transparency, but we urge that companies and CRO consider whether older public residential addresses should be redacted or replaced with contact addresses — especially where the directors are no longer active, or where a safety concern is established.

Section B: Proposed changes to the Co-operative Societies Bill:

Implications for information retained by a Co-operative Society:

Question B1: **Do you have any views on the intended approach relating to the maintenance by co-operative societies of address details of relevant officers?**
Response: Lionheart Governance Ireland supports the proposed approach for co-operative societies whereby a “contact address” (which may be the registered office or another suitable address) replaces the “usual residential address” on the publicly available Register of Directors and Secretaries. This matches the model for companies and protects personal data while ensuring there remains an avenue for service of documents and legal process via the retained but non-public “usual residential address. In our view, this is a balanced and proportionate approach and should be adopted.

Implications of the proposed changes for information maintained by the Registrar of Co-operative Societies:

Question B2: **Do you have any views on the intended approach relating to the filing with, and maintenance by, the Registrar of Co-operative Societies of address details of relevant officers of co-operative societies?**

Response: Yes. It is reasonable that the Registrar should continue to receive full "usual residential address" data in confidential form, even if it is not publicly published. This allows co-operative societies to satisfy legitimate legal, regulatory or enforcement functions (e.g., service of process, oversight, accountability) while guarding privacy and personal security.

However, we emphasise that the Registrar and co-operative societies must implement robust safeguards (data minimisation, secure storage, controlled access) in line with data-protection best practice (e.g. GDPR), to limit risk of misuse or unauthorised disclosure.

Restricted access to the "usual residential address":

Question B3:

Do you have any views on the proposed list of entities that may be granted access to the "usual residential address" of relevant officers of co-operative societies?

Response: Lionheart considers the proposed list — reflecting the "Tier 1" users under existing beneficial-ownership regimes — broadly appropriate. This includes law enforcement, regulatory, tax, and relevant professional-regulatory bodies.

We support restricting access to those entities with a legitimate public interest, regulatory or enforcement remit. That said, we advocate for the inclusion of procedural safeguards before disclosure (e.g., formal request, evidence of legitimate interest, audit-logging, confidentiality undertakings).

Question B4:

Are there any other comments you wish to make on the proposed approach to dealing with the "usual residential address" of relevant officers of co-operative societies?

Response:

Yes. In addition to the above:

- The legislation should explicitly limit the permitted uses of "usual residential address" data (e.g., service of legal process; regulatory/enforcement investigations) and prohibit secondary, non-essential uses (e.g., marketing, profiling, unsolicited contact).
- Given the sensitivity of personal address data, there should be a mechanism for periodic review or purge of address information where no longer needed or after an extended period of inactivity — particularly for officers no longer associated with the co-operative.
- For historical filings (before implementation), co-operative societies (or the Registrar) should consider whether older publicly-available residential addresses should be redacted or replaced with contact addresses — especially where safety or privacy concerns may arise.

Section C: Changes to the Registration of Limited Partnerships and Business Names Bill:

Implications for information retained by the LP:

Question C1: In relation to the implications for Limited Partnerships, do you have any comments on the proposals?
Response: Lionheart supports applying the same "contact address + retained usual residential address (non-public)" model to natural-person partners of LPs as is proposed for company officers. This maintains consistency across entity types and ensures privacy protections for individuals, while preserving the ability for legitimate legal/regulatory access. Such alignment is sensible; limited partnerships often involve small businesses or closely held structures, and exposing personal residential addresses publicly may disproportionately impact privacy and safety of individuals and their families.

Implications of the proposed changes for information on LPs maintained by the Registrar of Companies:

Question C2: **Do you have any views on the intended approach relating to the filing with, and maintenance by, the Registrar of Companies of address details of a partner in a Limited Partnership?**

Response:

Yes. We agree that the Registrar should retain the “usual residential address” in confidential form, and only the “contact address” (registered office or other suitable address) should appear on the public register. This ensures that LPs remain accountable and serviceable while respecting privacy.

As with companies and co-operatives, data-protection safeguards should be codified: secure storage, restricted access, data-use limitations and regular review.

Implications of the proposed changes for information on Register of Business names maintained by the Registrar of Companies:

Question C3:

Do you have any views on the intended approach relating to the filing with, and maintenance by, the Registrar of Companies of address details of a person registering a business name?

Response: Yes. For persons registering a business name, the same “contact address + private usual residential address” approach should apply. This is particularly important because many business-name registrants may operate sole businesses, or family enterprises, where public disclosure of residential address could pose undue privacy or security risks.
In our view, exposing only a contact address publicly is sufficient for the purposes of transparency, service and regulatory compliance.

Restricted access to the "usual residential address" for an LP and a registered business name:

Question C4: **Do you have any views on the proposed list of entities that may be granted access to the "usual residential address" of a partner of a Limited Partnership or a registered business name applicant?**
Response: Lionheart considers the proposed list (aligned with "Tier 1" users in beneficial-ownership regimes) appropriate for LPs and business-name registrants. Disclosure should be limited to entities with legitimate enforcement, regulatory, tax or judicial needs. We again urge that disclosure be conditional on a formal request, evidence of legitimate interest, and subject to audit, confidentiality and purpose-limitation constraints.

Question C5: **Are there any other comments you wish to make on the proposed approach to dealing with the "usual residential address" of a partner of a Limited Partnership or a registered business name applicant?**
Response: Yes. Additional observations: • The legislation should clearly define and limit acceptable purpose-uses for the residential-address data (e.g. service of process; regulatory enforcement), and prohibit secondary use (direct marketing, profiling, public distribution). • Given the higher risk for individuals using LP or business-name structures (often smaller, closely held or family-owned), there should be an option for affected persons to request that historical publicly available residential address data be replaced by contact addresses where safety, privacy or family-vulnerability considerations arise.

- The statutory regime should embed a data-protection governance framework: secure storage, restricted access, retention-period limitations, audit logging, and a clear procedural path for legitimate access requests — in line with GDPR's principles of data minimisation and purpose limitation.

Freedom of Information Act 2014 and Publication of Submissions

Your attention is drawn to the fact that information provided by you in submissions is subject to release by the Department under the Freedom of Information Act 2014. In responding to

this public consultation, all individuals and organisations should clearly indicate where their submission contains personal information, commercially sensitive information, or confidential information which they would not wish to be made publicly available by being published on the Department's website or released by the Department pursuant to the receipt of an FOI Request under the Freedom of Information Act 2014.

General Data Protection Regulation (GDPR) and Data Protection Acts 1988 to 2018

The Department of Enterprise, Tourism and Employment is subject to the provisions of the GDPR and Data Protection Acts 1988 to 2018. In this context, the Department will treat all personal information which you provide in submissions as part of this public consultation process with the highest standards of security in line with our data protection compliance requirements. We would like to draw your attention to the Department's Data Protection Privacy Notice which is available on our website and explains how and when we collect personal data, why we do so and how we treat this information. It also explains your rights in relation to the collection of your personal information and how you can exercise your rights under data protection laws.

November 2025