Insurance Ireland Comments on EDPB Template for Data Breach Notifications

Ireland is a leading global hub for insurance, reinsurance, and InsurTech, employing 43,000 people in Ireland, serving over 20 million customers and in more than 70 countries. Our members contribute €2.7 billion annually to the Irish Exchequer and pays more than €74 billion annually in claims, as well as safeguarding €300 billion of Life and Pensions assets.

Ireland is the number two provider of cross-border Life and Non-Life insurance in the EU, the fourth largest insurance market, and one of the largest reinsurance markets in the EU.

The role of Insurance Ireland is to advocate on behalf of our members with policymakers and regulators in Ireland, Europe and Internationally; to promote the value our members create for individuals, the economy and society; and to help customers understand insurance products and services so that they can make informed choices.

Insurance Ireland welcomes the EDPB's initiative to develop a common template for personal data breach notifications under Article 33 GDPR. A harmonised template has the potential to enhance consistency across supervisory authorities, improve legal certainty for organisations operating across multiple Member States and facilitate more efficient handling of personal data breach notifications.

Insurance Ireland supports the EDPB's objective of harmonising personal data breach notifications across the EU. To best facilitate this harmonisation, the final template should facilitate GDPR compliance without imposing unnecessary administrative burdens on controllers. Proportionality and recognition of the operational realities of incident response must be central to the final template. Insurance Ireland would like to draw the EDPB's attention to areas of the proposed template that could be further refined to achieve this.

Ensuring proportionality and reducing administrative burden

Insurance Ireland recognises that detailed information can support supervisory authorities' assessment of a data breach. However, the proposed template is excessively lengthy and granular. Insurance Ireland encourages the EDPB to review whether all requested information is strictly necessary for the purposes of Article 33 GDPR. The EDPB should simplify sections that do not materially contribute to the assessment of the incident.

Preserving a staged notification approach

The template should also make it clearer that controllers may submit an initial notification within the 72-hour period based on the information reasonably available at that stage, with additional details subsequently provided through follow-up notifications as many breaches, especially cybersecurity incidents and incidents involving processors or third-party service providers, require extensive technical investigation before reliable information becomes available. Further clarification would be beneficial regarding the practical operation of incomplete and follow-up notifications, including

whether information already submitted will be pre-populated in subsequent submissions and how controllers are expected to indicate where information remains under investigation.

Providing sufficient flexibility

The use of predefined categories can support harmonisation and facilitate consistent reporting. However, the template should retain sufficient flexibility through "Other", "Additional information" and free-text fields to accommodate the wide range of incidents encountered in practice.

Supporting consistency

A glossary of key terms and definitions should be included within the template or accompanying guidance. This would help ensure consistent interpretation across sectors and Member States and reduce the risk of divergent reporting practice or expectations.

Bulk notifications

Insurance Ireland encourages the EDPB to explore how the template could support the reporting or administration of multiple substantially similar breaches through a streamlined or bulk-reporting approach where appropriate. This could further reduce administrative burden while maintaining effective supervision.

Trivial Errors

Though the options available in Fields 60 *Nature of the incident* and 61 *Cause of the personal data breach*, the proposed template does not ease the burden of reporting for trivial accidental errors. Non-malicious internal errors remain included, as well as simple mix up of records.

Volume Threshold

There is no volume threshold and the proposed form does not effectively differentiate in terms of burden for between a single impacted data subject or a larger systemic incident. Insurance Ireland would welcome a *de minimis* threshold, or simplified reporting for very small numbers of impacted data subjects, where the impact is to less than 10 individuals.

Detailed feedback on the template

Finally, Insurance Ireland would like to provide the following feedback on the various parts of the template:

- **Field 26:** The confirmation regarding the accuracy of the information and the responsibility ("liability") is placed at the end of the address section. It may create the impression that the declaration applies only to the information provided in the address section (up to line 26), rather than to the information contained in the remainder of the notification form. In addition, the reference to the information pursuant to Article 13 of the GDPR is unclear.
- **Field 14–18:** The information requested in this section is mostly not required for the notification itself or for the assessment of the personal data breach. Considering the size of

the template, queries should be limited to what is strictly necessary. Furthermore, in field 17 an "Other" field is missing for organisations that do not fit into any of the listed classifications.

- **Section 2.1 to 2.4:** These sections request the contact details of up to five different contact persons (fields 13, 22, 31, 36 and 41). The contact details of one competent contact person should be sufficient and would also be more effective for any necessary communication.
- **Fields 55-57:** The new template does not differentiate between (i) confidentiality breaches through simple accidental disclosures to an unrelated third party and (ii) confidentiality breaches by a bad actor/cyber-attack.
- **Field 57 a)**: In this case, no notification would be required, as protection continues to be ensured (see Guidelines 01/2021, e. g. 5.1, Case No. 10).
- **Field 62:** Since the template already requests a short description of the nature of the breach, including detection, awareness, cause, measures in place and, where possible, the root cause, it would be useful to provide further guidance on the expected level of detail.
- **Field 63:** The template requests detailed information on the systems, software, services and infrastructures involved. It should clarify the level of detail expected at the initial notification stage, particularly where the root cause, affected systems, security measures or related documentation are still being investigated or not reasonably available at that time.
- **Fields 72 and 73:** The fields are not immediately clear. Compiling complex data within the reporting deadline entails a significant amount of extra work, which yields only minimal added value.
- **Field 87:** The notification requirements for Minor impacts should be removed in the interest of proportionality.
- **Field 125:** The categorisation of the documents does not seem feasible since the documents submitted relate to individual cases and do not always fit into specific categories.