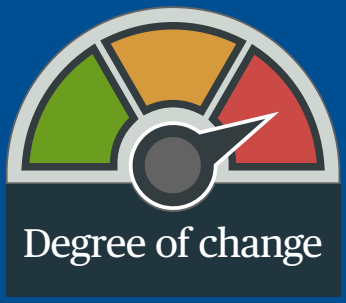
Personal data breaches and notification

At a glance

- Data controllers and data processors are now subject to a general personal data breach notification regime.
- Data processors must report personal data breaches to data controllers.
- Data controllers must report personal data breaches to their supervisory authority and in some cases, affected data subjects, in each case following specific GDPR provisions.
- Data controllers must maintain an internal breach register.
- Non-compliance can lead to an administrative fine up to €10,000,000 or in case of an undertaking, up to 2% of the total worldwide annual turnover of the preceding financial year, whichever is higher.
- As things stand, the specific breach notification regime for communications service providers, set out in Commission Regulation 611/2013 on the measures applicable to the notification of personal data breaches under Directive 2002/58/EC, still applies.

To do list

- ☐ In line with the accountability principle laid down by the GDPR, data controllers and data processors should develop or update their internal breach notification procedures, including incident identification systems and incident response plans.
- ☐ Such procedures should be regularly tested and re-reviewed.
- ☐ Work with your IT/IS teams to make sure they implement appropriate technical and organisational measures to render the data unintelligible in case of unauthorised access.
- ☐ Insurance policies should be revisited to assess the extent of their coverage in case of breaches.
- ☐ Template MSA/data protection clauses and tender documentation should be updated by customers, including: (i) to require suppliers to proactively notify breaches to them; and (ii) put a great emphasis on the duty to cooperate between the parties.



Incidents which trigger notification

In case of an incident defined as, *"a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed"*, the new breach notification regime under the GDPR will apply as follows:

1. Obligation for data processors to notify data controllers

Timing:

Without undue delay after becoming aware of it.

Exemption:

None in the GDPR (but EDPB tasked to issue guidelines on *"the particular circumstances in which a controller or a processor is required to notify the personal data breach"*).

Observations:

- All breaches will have to be reported.
- EDPB to issue guidelines to clarify the notion of "undue delay" and the particular circumstances in which a data processor is required to notify the personal data breach.

2. Obligation for data controllers to notify the supervisory authority

Timing:

Without undue delay and, where feasible, not later than 72 hours after becoming aware of it.

Exemption:

No reporting if the breach is unlikely to result in a risk to the rights and freedoms of natural persons.

Observations:

- When the timing obligation is not met, reasons will have to be provided to the supervisory authority (e.g. request from a law enforcement authority).
- EDPB to issue guidelines to clarify the notion of "undue delay" and the particular circumstances in which a data controller is required to notify the personal data breach.

3. Obligation for data controller to communicate a personal data breach to data subjects

If the data controller is yet to do so, the supervisory authority may compel the data controller to communicate a personal data breach with affected data subjects unless one of the three exemptions is satisfied.

Timing:

Without undue delay: the need to mitigate an immediate risk of damage would call for a prompt communication with data subjects whereas the need to implement appropriate measures against continuing or similar data breaches may justify more time for communication.

Exemption:

No reporting if:

- The breach is unlikely to result in a high risk for the rights and freedoms of data subjects;
- Appropriate technical and organisational protection were in place at the time of the incident (e.g. encrypted data); or
- This would trigger disproportionate efforts (instead a public information campaign or "similar measures" should be relied on so that affected individuals can be effectively informed).

Documentation requirements

- Internal breach register: obligation for the data controller to document each incident *"comprising the facts relating to the personal data breach, its effects and the remedial action taken"*. The supervisory authority can be requested to assess how data controllers comply with their data breach notification obligations.
- There are also prescribed requirements to satisfy in the communication to the supervisory authority (e.g. describing the nature of the personal data breach, including, where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of data records concerned, etc.) and the communication to affected individuals (e.g. describe in clear and plain language the nature of the personal data breach and provide at least the following information: (i) the name and contact details of the Data Protection Officer or other contact point where more information can be obtained; (ii) the likely consequences of the personal data breach; and (iii) the measures taken or proposed to be taken by the data controller to address the personal data breach, including, where appropriate, to mitigate its possible adverse effects).

Sanctions in case of non-compliance

Failure to meet the above requirements exposes the organisation to an administrative fine of up to €10,000,000 or in case of an undertaking, up to 2% of the total worldwide annual turnover of the preceding financial year, whichever is higher.

What about the other EU breach notification regime for communications service providers?

As things stand, Regulation 611/2013 – which details a specific procedure for breach notification (laid out in Directive 2002/58/EC (the "e-Privacy Directive") as amended) - still applies to providers of publicly available telecommunications services (e.g. telecommunication companies, ISPs and email providers). However, on 10 January 2017, the European Commission published its proposed text for the new e-Privacy Regulation.

The fact that this Regulation will enter into force on the same date as the GDPR – 25 May 2018 – symbolises the intended harmonious relationship between the two Regulations. The text repeals the e-Privacy Directive but contains very similar wording to the applicable breach notification wording in that Directive. This being said, the text does not repeal Regulation 611/2013. Therefore, technically, telecoms providers will have to notify breaches to the competent DPAs following the regime established under Regulation 613/2013, and not under the GDPR. However, we believe that at some point, Regulation 613/2013 will be repealed in favour of the regime under the GDPR.

Where can I find this?

Recitals 85-88 *Articles 33, 34, 70, 83 & 84*