N O V E

GUIDELINES ON DATA BREACH NOTIFICATIONS & PROFILING

SUMMARY REPORT

OVERVIEW

On October 17, the Article 29 Working Party (29WP) released draft guidelines on data breach notifications and on profiling. **A consultation is now open until November 28 for stakeholders to participate.** The 29WP will consider this input before a final version is adopted. By February 2018, all guidelines, including on breach reporting and profiling will have to be finalised. In May 2018, the GDPR becomes applicable and the 29WP will become the European Data Protection Board (EDPB) formally adopting these texts (without changes).

GUIDELINES ON DATA BREACH NOTIFICATIONS

Data controllers are required to notify the competent Supervisory Authority (SA) about personal data breaches within 72 hours unless "the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons". Additionally, in case the breach has a "high risk to the rights and freedoms of natural persons", they will have to be communicated to the data subject without undue delay. The data processor has to report personal data breaches to the data controller once it is aware, but not to the authorities or individuals.

Failing to comply with these rules could lead to sanctions or administrative fines of up to EUR 10 million or 2% of the data controller's global annual turnover.

AWARENESS

Time starts to run from the moment the controller/processor becomes aware of the breach, but what does "aware" mean? According to the guidance, it means that there is a "reasonable degree of certainty that a security incident has occurred that has led to personal data being compromised". While in some cases awareness might be there from the offset, in others a reasonable degree of certainty is only achieved following an investigation, which needs to start as soon as possible. During these preliminary stages, the data controller is not considered to be aware.

The data processor should notify data controllers of breaches "without undue delay". The GDPR does not provide an explicit time limit within which the processor must alert the controller, except that it must do so "without undue delay". The 29WP recommends however an immediate notification by the processor to the controller, with further information about the breach provided in phases as information becomes available.

NOTIFICATION IN PHASES

Notification in phases is allowed, particularly since "full and comprehensive details of the incident may not always be available" within 72 hours. When notifying the SA, the controller should inform that more information will be provided at a later point.

As the focus in breach notification procedures is a quick response, more comprehensive investigations on breaches can follow a shorter preliminary investigation that leads to a "reasonable degree of certainty". A controller may therefore update the SA of any evidence

gathered in a follow-up investigation. As stated in the guidelines "there is no penalty for reporting an incident that ultimately transpires not to be a breach".

DELAYED NOTIFICATION

In case the 72h timeline is missed, a delayed notification may be exceptionally allowed if duly justified. The guidelines give the following example: if a controller experiences "multiple, similar confidentiality breaches over a short period of time, affecting large numbers of data subjects in the same way", it may submit a single bundled notification representing all the breaches more than 72 hours after first becoming aware of them.

SUPERVISORY AUTHORITY

In case of an incident in cross-border data processing with the breach affecting individuals in more than one Member State, the data controller will need to notify the lead SA. The identification of the lead has already been subject to guidance in already approved 29WP guidelines. Should the data controller still fail to identify the lead, at a minimum, it needs to notify the local authority where the breach has taken place.

The 29WP also suggests that the controller may *choose* to notify authorities in other Member States where individuals are affected. If the controller chooses not to do this, then it should advise the lead authority in which other Member States individuals are likely to be affected.

BREACHES THAT DO NOT NEED TO BE REPORTED TO SUPERVISORY AUTHORITY

As stated in the GDPR, breaches that are "unlikely to result in a risk to the rights and freedoms of natural persons" do not need to be reported. The 29WP guidelines address these incidents by way of examples:

- A breach involving data which is already publicly available, where there is no likely risk to individuals would not need to be notified
- A loss of encrypted data would not need to be reported – provided that the key is held securely and that the encryption was operational when the device was lost. (Some devices have encryption which is only active when the device is turned off; others are more sophisticated). Any decision not to report due to use of encryption should be revisited if facts change – for example, if it turns out that key management was not secure.

Even if notification is not required initially, "this may change over time and the risk would have to be re-evaluated." For example, if the key turns out to have been compromised, or a malfunction is detected in the encryption software, then notification would be required.

BREACHES THAT SHOULD NOT BE REPORTED TO THE DATA SUBJECT

To avoid fatigue, notifying the data subject should only occur if the breach poses a "high risk". Certain conditions are also set forth in the GDPR that exempt the need to report. The SA may however require the data controller to notify the data subjects if it considers that the breach is likely to present a high risk to data subjects.

RISK TO THE RIGHTS AND FREEDOMS OF THE DATA SUBJECT

The guidelines say that the "risk to the rights and freedoms of individuals" is the "key trigger" for the notification requirement to the SA, while "high risk to the rights and freedoms of individuals" is the "key trigger" for communication to data subjects.

Risks result from breaches that lead to "physical, material or non-material damage for the individuals whose data have been breached". If it involves personal data that reveals special

categories of data, such as racial or ethnic origin or political opinions, this is deemed to be high risk. The guidelines recommend that risk assessment should consider the following criteria:

- Type of breach;
- Nature, sensitivity, and volume of personal data;
- Ease of identification of individuals;
- Severity of consequences for individuals;
- Special characteristics of individuals (e.g., children);
- Number of affected individuals;
- Special characteristics of the data controller.

GUIDELINES ON AUTOMATED DECISION-MAKING AND PROFILING

Profiling is a "procedure which may involve a series of statistical deductions (...) often used to make predictions about people". This means that "simply assessing or classifying individuals based on characteristics" could be considered profiling, even without a predictive purpose.

AUTOMATED DECISION-MAKING

The guidelines define automated decision-making as "the ability to make decisions by technological means without human involvement." It can take place with or without profiling, and can be based on any type of data.

PROHIBITION

Art 22(1) of the GDPR prohibits fully automated individual decision-making, including profiling that has a legal or similarly significant effect. The guidelines clarify if a recommendation about a data subject is produced by an automated process but reviewed by a human being who "takes into account other factors in making the final decision". This involvement also has to be meaningful and by someone who is competent to decide.

LEGAL AND SIMILARLY SIGNIFICANT EFFECTS

Legal effects are those that have an impact on an individual's legal rights such as statutory or contractual rights (for example an individual being refused entry at a border, being denied a social benefit granted at law or having their mobile phone terminated for failure to pay the bill).

Similarly significant effects are those that are equivalent or similarly significant to legal effects. The effect must be more than trivial and must have the potential to significantly influence the circumstances, behaviour or choices of the individuals concerned (examples could include automatic refusal of an online credit application or e-recruiting practices without human intervention).

The guidelines also expand on online advertisement. This practice may qualify as having significant effects on the data subject depending on the following characteristics:

- The intrusiveness of the profiling process;
- The expectations and wishes of the individuals concerned;
- The way the ad is delivered;
- The particular vulnerabilities of the data subjects targeted.

EXCEPTIONS

The guidelines address the exceptions mentioned in Art 22 of the GDPR. It enumerates a list of legal bases for profiling that do not all apply to automated decision-making:

- With subject's explicit consent.
- Necessary for the performance of a contract.
- Necessary for compliance with a legal obligation.
- Necessary to protect vital interests.
- Necessary for the performance of a task carried out in the public interest or exercise of official authority.
- Necessary for the legitimate interests pursued by the controller or third party.

The guidelines emphasise that Art 22 requires explicit consent and the risk for the data subject in this context is considered high. Explicit consent will be addressed in future guidelines on consent.

As for the "necessity for performance of a contract" exception, the guidelines clarify that simply including profiling in the small print of an otherwise unrelated contract does not fulfil the minimum requirements to use this option.

Under Article 6(1)(f) the legitimate interests of a controller or third party may provide a basis for profiling. Determining if this is so requires balancing those interests against the data subjects' interests, fundamental rights, and freedoms; the guidelines suggest the following criteria:

- The level of detail of the profile.
- The comprehensiveness of the profile.
- The impact of the profiling on the data subject.
- The safeguards aimed at ensuring fairness, non-discrimination, and accuracy in the profiling.

RIGHTS OF THE DATA SUBJECT

These guidelines specifically address the following rights:

- Right to be informed: data controllers are instructed to "find simple ways to tell the data subject about the rationale behind, or the criteria relied on in reaching the decision" by providing information "meaningful to the data subject."
- Right of access: the data subject has the right to obtain details of any personal data used for profiling, including the categories of data used to construct a profile. In addition to information about the profile, the controller should make available the data used as input to create the profile.
- Right not to be subject to a decision based solely on automated decision-making: data controllers must act affirmatively to provide data subjects with access to "at least the right of human intervention,". A simple way must be provided to the data subject to access these rights enabling the individual to express his or her view and contest a decision.
- Right to object: according to the guidelines, there is a need for affirmative conduct by the data controller to inform data subjects of the right to object, and the need for a quick reply if a subject exercises that right. Controllers are required to interrupt profiling unless able to demonstrate "compelling legitimate grounds" that outweigh the interests, rights and freedoms of the data subject. It is about "profiling [that is] beneficial to society at large" and "not just the business interests of the controller". Controllers must show two specific additional elements to continue profiling over a subject's objection: (i) the impact to the data subject is limited to the minimum necessary to meet the particular objective, (ii) the objective is critical for the organization. Data subjects have an unconditional right to object to processing for direct marketing purposes.

FURTHER PROCESSING

Additional processing is permitted depending on:

- Relationship between the purposes for which the data were collected and the purposes of further processing.
- Context in which the data were collected and the reasonable expectations of the data subjects.
- Nature of the data and the impact of further processing on the data subjects.
- Safeguards applied by the controller to ensure fair processing and avoid undue impact on the data subject.

CHILDREN AND PROFILING

Recital 71 GDPR provides that significant automated decision making (including profiling) should not concern children. The 29WP does not consider this an absolute prohibition, as the restriction is in the recitals and not the main text. Accordingly, the guidelines give examples where there may be circumstances where data controllers need to carry out significant automated decisions in relation to children.