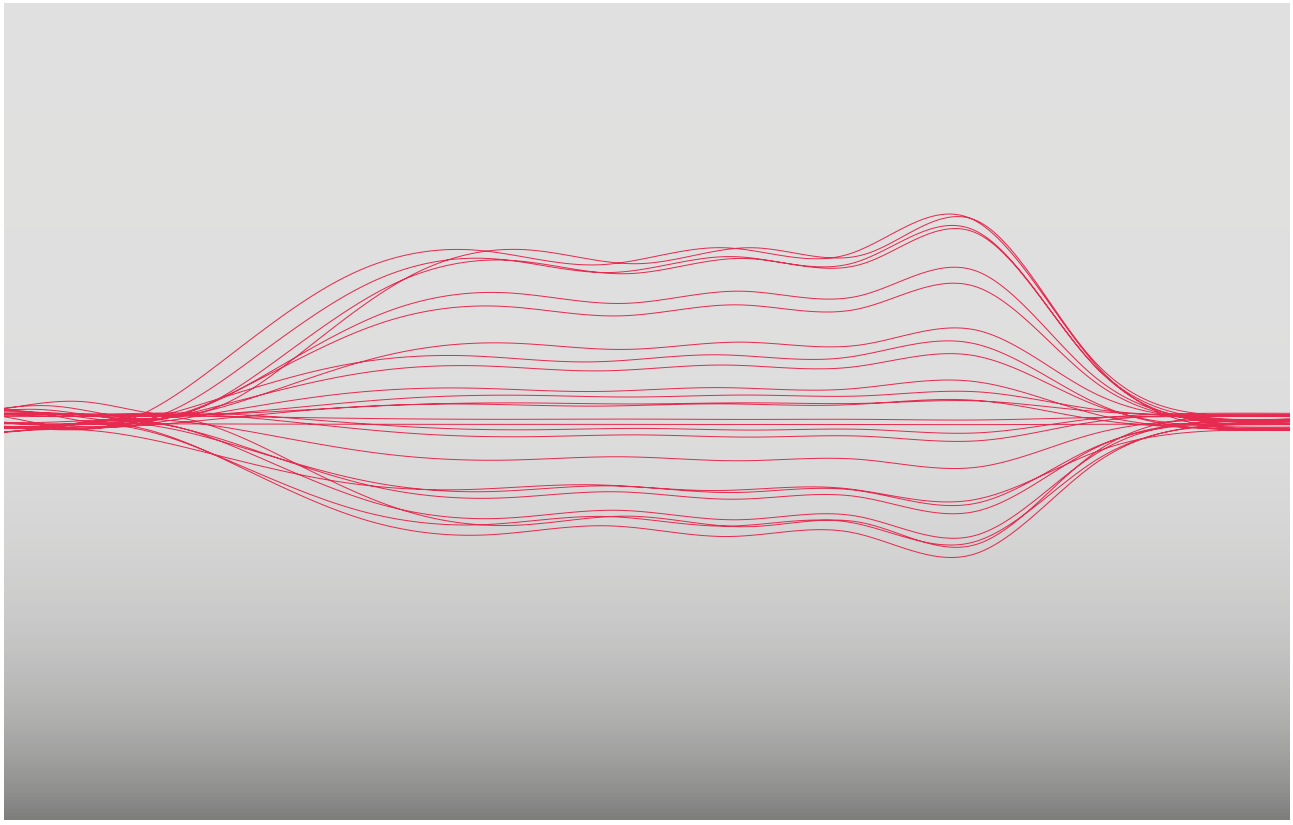

NOTIFY – DLA Piper's Data Breach Assessment Tool

Under the General Data Protection Regulation (GDPR), organisations are required to notify personal data breaches to the supervisory authority, unless the breach is unlikely to result in a "risk" to the rights and freedoms of the affected individuals. If, however, the breach is likely to result in a "high risk", the affected individuals themselves need to be informed.

But how can an organisation determine the level of risk?

As there is little guidance and typically a lot of time pressure, organisations may be tempted to rely on their gut feeling. Yet this subjective and inconsistent approach creates a risk for the organisation, due to the possibility of fines for non-compliance with notification requirements. In addition, supervisory authorities demand consistency in an organisation's approach.

Faced with these challenges, organisations need a consistent methodology, based on objective and quantitative criteria. This is where NOTIFY can assist.

NOTIFY is a tool built by DLA Piper that combines elements from three official sources: ENISA, the GDPR and the EDPB. NOTIFY is structured as an intelligent questionnaire that calculates the level of risk dynamically.

DLA PIPER

Risk score: Very high

Based on information provided by CompanyX – calculation details on page 2.
For more information on risk classification and imapct for data subjects, see page 3.

4,25

Data processing context	x	Ease of identification	+	Circumstances of breach
4	x	1	+	0,25

However: Notification exemption

The data breach appears to quality for one notification exemption foreseen by the European Data Protection Board: Unintelligible data & backups available

It allows DLA Piper's lawyers, as well as its clients, to carry out their assessments of data breaches in a **consistent** and **objective** manner. NOTIFY also generates a **report** summarising the outcome of the assessment, resulting in easier communication. In addition, it helps organisations document the reasoning behind their decision, fully in line with the principle of accountability.

Clients can choose to use the tool themselves or to have DLA Piper carry out the relevant assessment, in which case the outcome is protected by **legal privilege.**

NOTIFY by DLA PIPER

Current risk score: 1.25 = 1 (Data Processing Context) * 1 (Ease of Identification) + 0.25 (Circumstances of Breach)
Additional criteria: Exempt from notification to supervisory authority as well as data subjects

Does the nature of the data set provide substantial insight into the data subject's situation? *[Example: a medical certificate stating that a data subject is "in good health" does not provide substantial insight into the data subject's health.]*	No	
Can (all) the affected data be collected easily (independently from the breach) through publicly available sources (e.g. combination of information from web searches)?	--select--	
Can the nature of this data lead only to general assumptions regarding the data subject's situation?	--select--	
Can the nature of this data lead only to assumptions about sensitive information?	--select-- (--select-- / Yes / No)	

<** Click the |+| button to view examples

1.5. Other information on data processing context

Beyond specific factors that are related to the kind of personal data that are affected by the breach, there are other factors to be taken into account. Please indicate whether any of the following elements are relevant to the processing and breach:

Risk classification applied*

RISK SCORING	RISK CLASSIFICATION	POSSIBLE IMPACT FOR THE DATA SUBJECT
Score < 2	Negligible	Data subjects either will not be affected or may encounter a few inconveniences, which they will overcome without any problem (time spent re-entering information, annoyances, irritations, etc.)
2 ≤ score < 3	Medium	Data subjects may encounter significant inconveniences, which they will be able to overcome despite a few difficulties (extra costs, denial of access to business services, fear, lack of understanding, stress, minor physical ailments, etc.).
3 ≤ score < 4	High	Data subjects may encounter significant consequences, which they should be able to overcome albeit with serious difficulties (misappropriation of funds, blacklisting by banks, property damage, loss of employment, subpoena, worsening of health, etc.).
Score > 4	Very high	Data subjects may encounter significant, or even irreversible, consequences, which they may not overcome (financial distress such as substantial debt or inability to work, long-term psychological or physical ailments, death, etc.).

** source: ENISA (2013)*

Some relevant terms

Availability breach: Data breach involving the temporary or permanent inaccessibility of data. The existence of backups can limit the severity of an availability breach.

Circumstances of breach: an evaluation of how the breach came about (confidentiality breach, integrity breach, availability breach) and how widespread the breach may be, as well as specific aggravating circumstances (malicious intent).

Confidentiality breach: Data breach involving access by unauthorized persons or by people without a legitimate purpose to access it. The severity of the confidentiality breach depends on the number and type of parties with unlawfully access.

Data processing context: categories of personal data affected by the breach and circumstances of processing (in order to determine whether a particular kind of processing presents an inherent risk).

Ease of identification: a measure to assess how easily the identity of the individuals concerned can be deduced from the data involved in the breach.

EDPB: European Data Protection Board, which has replaced the Article 29 Working Party (WP29). The EDPB has notably endorsed the WP29 Guidelines on Personal data breach notification (WP250 rev.01).

ENISA: European Union Agency for Network and Information Security, which published in 2013 its "Recommendations for a methodology of the assessment of severity of personal data breaches".

GDPR: Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

Integrity breach: data breach involving alteration and substitution of data in a manner that would have a negative impact on the data subject (more severe if likely that alteration could cause harm to the data subject).

Malicious intent: Assessment of the cause of the breach, in particular if the breach is due to error, mistake (e.g. loss, software bug, ...) or by an intentional action of malicious intent (e.g. theft, hacking, ransom demand, aim to harm processor or controller, ...). In case of malicious intent, it is more likely that the data is/will be used in harmful way.