Post-breach: The discretion in assessing the risk of harm

06

Justin Tivey
Partner
jtivey@dacbeachcroft.com

Becky Lea
Legal Director
blea@dacbeachcroft.com

Protection from the risk of harm is central to most data protection regimes. The clue is very much in the name after all: the General Data Protection Regulation, the Data Protection Act 2018 and so on.

Personal data breaches occur when there is a security breach leading to accidental or unlawful loss of confidentiality, integrity or availability of personal data being processed. A breach does not have to result from third party activity; accidental disclosures are as reportable as hacking incidents.

Preparatory tools such as Data Protection Impact Assessments (**DPIAs**) help identify, analyse and mitigate the risks to data subjects likely to arise from processing activities relating to their personal data.

However, if the worst happens, and a data breach occurs, then the assessment of risk arises again. Whether a controller must notify the regulator or affected individuals is determined by assessing the potential risk of harm to affected data subjects. This assessment is necessary to ensure compliance with regulatory requirements and to avoid the risk of possible enforcement activity by the regulator. Failures to notify can attract regulatory investigations, reprimands and potentially fines of up to £17.5 million or 4% of total annual worldwide turnover, whichever is higher.

The legislative background and guidance

The two key statutory provisions within the UK GDPR for post-breach considerations are as follows:

Article 33(1):

"In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to* [the regulator], *unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons."

Article 34(1):

"When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay."

How does a controller decide if a breach is unlikely to result in a risk and thus is not notifiable to the regulator or, in the alternative, that the breach is likely to result in a high risk and should be communicated to data subjects themselves?

Both the UK data protection regulator, the Information Commissioner's Office (**ICO**) and the European Data Protection Board (**EDPB**) have issued guidance about how to make this assessment, even including a mathematical formula! Controllers need to consider how straightforward this guidance is to use and whether risk and harm assessments allow for subjectivity or are strictly formulaic.

The GDPR Recitals indicate the types of harm that might result from a data breach. Recital 85 highlights *'material'* and *'non-material'* damage and lists *'loss of control'* over personal data, *'limitation of rights'* and more specifically *'discrimination, identity theft or fraud, financial loss, reversal of pseudonymisation, reputational damage, loss of confidentiality of data protected by professional secrecy or any other significant economic or social disadvantage'*.

Recital 88 states that consideration should be given to the circumstances of the breach, including whether technical measures protecting data limits the likelihood of identity fraud or other misuse of the data.

These factors are good starting points in indicating the types of harm that controllers need to think about when assessing the risk to data subjects. However, there is a lot of room for interpretation in some of these concepts; limitation of rights, reputational damage and economic and social disadvantage in particular are capable of being interpreted widely or narrowly. One controller or data subject may see information as reputation-related, while another may not. How does the controller determine whether the risk of harm is unlikely, high, or somewhere in between?

Recital 75 also lists types of data which might give rise to risk including special category data, data evaluating data subjects, data relating to vulnerable people and large datasets. Recital 76 refers to the likelihood and severity of the risk to data subjects but only to state that the risk should be determined *'by reference to the nature, scope, context and purposes of the processing'* and that risk *'should be evaluated on the basis of an objective assessment, by which it is established whether data processing operations involve a risk or a high risk'*.

Recital 77 goes on to suggest that guidance as regards the identification of the risk related to processing and assessment of the likelihood and severity could be provided by means of guidelines provided by the EDPB. The EDPB may also issue guidelines on processing operations unlikely to pose high risks to individuals' rights and freedoms. To date, the EDPB has issued guidance on these types of operations via binding opinions such as Opinion 6/2024 on processing operations exempt from the data protection impact assessment requirements.

The regulatory guidance

The ICO advises controllers to implement strong breach detection and reporting procedures to help determine if they must notify authorities or affected individuals about a data breach. The guidance starts by referencing the Recitals of the UK GDPR mentioned above. The ICO recommends that the focus should be on any potential negative consequences for individuals, particularly if the breach is not addressed appropriately. On becoming aware of a breach, the controller should contain it and assess the potential adverse consequences for individuals, based on how serious or substantial these are, and how likely they are to happen.

The ICO also recommends consulting risk section IV of the Article 29 Working Party Guidelines (now the EDPB) on personal data breach notification, now identified as Guidelines 9/2022. Drafted in anticipation of the implementation of the GDPR and adopted on 3 October 2017 and updated in 2018. 2022 and 2023, these are a useful reference point.

The Guidelines repeat the Articles and Recitals referred to above but add assumptions that where special category data is involved, then damage to data subjects should be considered "likely to occur". The need to evaluate likelihood and severity of risk, and to make an objective assessment, is also emphasised. The difference between a DPIA and breach assessment is also highlighted, noting that the DPIA considers hypothetical situations, whereas a breach scenario is in the context of an actual event.

The EDPB Guidelines also highlight assessment criteria to help the thought process for the controller. The key criteria being:

- **The type of breach:** For example, a breach involving the disclosure of data to a third party may create more risk than one where data is simply lost.
- **The nature, sensitivity and volume of data:** The relevance of these criteria is self explanatory, but the guidance highlights greater risk if different types of data can be combined to create an identity theft risk. Similarly, a large variety of data about one person or a large volume affecting many people will also increase risk.
- **The ease of identification of individuals:** Can a specific individual be identified from the data or with the data and other available information? If not, the risk is lowered. Similarly, encryption and pseudonymisation of data will lower the risk.
- **The severity of consequences to the data subjects:** Again, this speaks for itself, but the guidance also flags that if data is in the hands of a malicious party the risk will likely increase. Accidental disclosure to a third party who agrees to delete the data being at one end of the scale and unknown hackers at the other end. The duration of any adverse consequences is also a factor.
- **The characteristics of data subjects and controller:** These considerations are contextual. Children and vulnerable adults are obvious examples of data subjects at inherently greater risk. Controllers such as medical establishments are likely to have data which could cause harm if mishandled.
- **The number of affected individuals:** Although one individual can be seriously impacted, the guidance is that generally the higher the number of affected data subjects, the greater the impact of the breach.

Overall, the guidance confirms that, if in doubt, a controller should err on the side of caution and notify. Additional examples of scenarios and suggested appropriate notification outcomes are provided in the guidance, but it is far from a clear decision tree or formula.

The formulaic approach

Mathematics geeks may want to refer to the European Union Agency for Network and Information Security (**ENISA**) for guidance. ENISA has published a recommended methodology for the assessment of severity of personal data breaches. The methodology was developed in 2013 based on the legislation at that time, but with an eye to the then-developing GDPR.

The aim was to develop a quantitative tool to assess the severity of data breaches to assist in notification decisions. The tool identifies factors, scores them, then uses a formula to produce a 'severity score'. The factors fed in are the "Data Processing Context" (DPC); "Ease of Identification" (EI); and "Circumstances of the Breach" (CB). Each factor has a score. For example, a DPC score of 1 is given for simple biographical data but it could be increased to 2, 3 or 4 if that biographical data revealed more sensitive information such as behavioural data, financial data or special category data. By way of example, a database of professional CVs might be given a score of 1, but that database is owned by an organisation (i) helping the unemployed, then the score might increase to 2; or (ii) supporting recovering drug addicts find work, then the score might be increased to 4.

The Ease of Identification (EI) scores are 0.25, 0.5, 0.75 or 1, with the scores rising as identification of the data subject is deemed easier.

Finally, the Circumstances of the Breach (CB) scores are 0, 0.25 or 0.5. These are applied depending on whether the breach is a confidentiality breach, an integrity breach or an availability breach. A lost file might score 0, an email sent to a few known recipients in error might score 0.25 and data published to an unknown number of recipients, say on a webpage, might score 0.5.

The formula is: DPC x EI + CB = Severity score

Severity score of less than 2 are suggested to be low risk breaches, score of up to 3 are suggested to be medium risk breaches, scores of up to 4 are suggested to be high risk breaches and scores of 4 and above are suggested to be very high risk.

However, even such a formulaic approach should be subject to review to consider the specific circumstances in question. For example, other features of the breach such as the number of data subjects affected (larger numbers, in the methodology put at over 100, being seen as inherently greater risk) or unintelligibility of data (for example by encryption) before reaching a final assessment.

The role of discretion

Regulators warn against of over-notification, arguing it causes notification fatigue and unnecessary alarm. Unnecessary notifications can invite claims for compensation which would otherwise be avoided. Of course, seeking to avoid claims is in no way a legitimate basis for withholding notification when the established threshold has been reached.

In reality, there is a wide role for discretion to play in post-breach risk assessment. How risk is evaluated is often still a subjective exercise straining to be objectively reasonable.

This can be illustrated by the frequently encountered problem of exfiltration of the contents of HR files. These will comprise a range of data varying wildly from data subject to data subject. Although some studies have examined the market value of personal data on the dark web, the findings generally align with expectations; for example, scans of identity documents hold significant value, whereas information such as a national insurance number is typically less valuable. Similarly, your bank account number has little value but your bank account log on credentials does.

The problem for controllers is that there is no regulatory advice on what combinations of data will likely to give rise to identity theft. It is left to organisations to determine that question for themselves.

If a controller's data is encrypted, how strong does the encryption need to be for the data to be considered secure? Is a complex password necessary, or is higher-level security required? What is the level of effort hackers would invest in accessing numerous documents with uninformative labels if the password is just "1234"? Controllers and regulators often lack the expertise or motivation typical of cyber criminals.

It is also the case that there is often no proof of a correlation between say increased phishing emails being received by a data subject and a breach that has affected their data.

This means there is still a large element of interpretation of what constitutes a 'high risk' and what is 'likely.' The decision about whether to notify or not, involving reaching a rational decision about risk, should not prioritise the controller's interests over the data subject's, and must be capable of being justified if the decision is later called into question.

Alternative approaches

In some jurisdictions, for example some US states, certain items of data or combinations are designated as requiring notification. If a breach involves that data, then those data subjects must be notified. Discretion is all but eliminated.

Evolving standards & flexibility v certainty

The future of risk assessment is uncertain. We are not aware of any radical shifts in the pipeline, certainly in the UK. The current regime leads towards more detailed data and risk analysis, whereas a broad brush or formulaic process may miss the mark for data subjects or controllers. Currently, the main emphasis is on achieving the appropriate outcome for each data subject, which aligns with the core principles underpinning the data protection framework in the UK.