OMBUDSMAN
CAYMAN ISLANDS

Guidance on Monetary Penalty Order (MPO) Methodology

3 September 2021

Background

Section 55 of the Data Protection Act (2021 Revision) (DPA) grants the Ombudsman the power to issue a monetary penalty order (MPO) which is not to exceed $250,000.

In accordance with section 56 of the DPA, Guidance on Monetary Penalty Orders[1] was developed in consultation with the Cabinet. It lists factors for evaluating whether the Ombudsman should impose an MPO, and – if a penalty is to be imposed - factors for determining the amount of the penalty.

The Office of the Ombudsman uses two additional tools to assist in the evaluation and determination of an MPO:

a) Breach Severity Assessment Tool; and
b) Matrix for Monetary Penalty Calculation.

This Guidance seeks to explain these two additional tools. It should be read in conjunction with the broader Guidance on Monetary Penalty Orders issued under section 56.

The factors taken into account in evaluating whether to impose an MPO, determining the amount of an MPO, and applying these tools to the circumstances of a specific infringement are listed in the Notice of Intent that is sent to the data controller in accordance with sections 55(5) to (7) of the DPA.

a) Breach Severity Assessment Tool

This tool is a spreadsheet that captures relevant characteristics of a specific personal data breach, and assists in the assessment of the severity of the breach.

This tool is based on the "Recommendations for a methodology of the assessment of severity of personal data breaches" of the European Union's Agency for Network and Information Security (ENISA),[2] which are used by a number of international data protection authorities such as the UK's Information Commissioner's Office (ICO).

[1] See: https://ombudsman.ky/images/pdf/OMB_DP_Guidance_on_Monetary_Penalties.pdf.

[2] European Union Agency for Network and Information Security, Recommendations for a Methodology of the Assessment of Severity of Personal Data Breaches. Working Document, v.1.0, December 2013, https://www.enisa.europa.eu/publications/dbn-severity/at_download/fullReport.

In line with the ENISA methodology, three core elements are taken into account when the tool calculates the breach severity score: the type of data, the ease of identification of individuals, and the circumstances of the breach. See Appendix 1 for a listing of options in each category.

Each option on the calculation sheet is given a weighting which automatically feeds into the total breach severity score calculation at the bottom of the sheet. This total score equates to a severity rating of Low, Medium, High or Very High, which is colour-coded from green (low severity) to red (very high severity).

We use this score as an indicative, but not definitive measure of the severity of the breach. We always take account of the particular context or circumstances of a breach on a case-by-case basis, so our final decision may differ from the score given by this tool. However, if our final decision is greatly different to the conclusion from this tool, we must explain our reasoning for this.

Each element of the tool is explained in the instructions provided with the calculation sheet, along with definitions of the options to guide our responses. The tool also refers back to the ENISA document which contains further detailed guidance, including worked examples, to help us determine the appropriate levels for each of the elements. This tool is intended to be used in conjunction with the Annexes in the ENISA document, to fully inform our decisions.

b) Matrix for Monetary Penalty Calculation

This second tool is based on the methodology employed by the UK's Information Commissioner's Office (ICO).[3] This tool assists the determination of the amount of the penalty, in situations where a determination has been made that an MPO will be imposed.

It consists of a matrix along two axes: the horizontal axis represents the seriousness of the contravention, and the vertical axis the level of culpability of the data controller.

The level of **severity** or seriousness of the contravention is considered in terms of the nature of the personal data concerned and the number of individuals actually or potentially affected, as entered into the Breach Severity Assessment Tool (see above).

The level of **culpability** will depend on:

- whether the contravention was caused or exacerbated by activities or circumstances within or outside the direct control of the data controller concerned. Note that the data controller will be held accountable for the actions of any data processor they have engaged;
- whether procedures or processes were in place to avoid the contravention;
- whether any steps were taken to avoid the contravention (e.g. staff training).

Each cell in the matrix represents a starting amount for a monetary penalty. For instance, a contravention of the DPA with a level of seriousness of "1" (score of 3.0 – 3.5) and no or low culpability of the data controller, has a penalty level with a starting point of $5,000. On the other hand, a contravention with a higher level of seriousness of "3" (score of 4.5 – 5.0) and a high culpability will

[3] For references, see Appendix 3 below.

carry a penalty with a starting point of $165,000. The starting level of the monetary penalty is then adjusted in accordance with applicable aggravating and mitigating factors, as further explained below.

Note that only breaches with a high or very high level of seriousness (score of 3.0 or above) are likely to attract a monetary penalty, although exceptions may occur depending on the context.

For a copy of the matrix, see Appendix 2 below.

Aggravating and mitigating factors used in MPO calculations

The type of individuals affected (e.g. were any vulnerable individuals or children involved?)	0% to +25%
Whether the contravention was a 'one-off' event, or part of a series of similar contraventions	0% to +30%
The duration and extent of the contravention	0% to + 30%
Whether any steps were taken once the data controller became aware of the contravention, both positive (e.g. voluntary reporting to the Ombudsman) or negative (concealment of the contravention)	-25% to + 25%
Whether the data controller had been willing to offer compensation to the individuals affected	-20% to 0%
The degree of cooperation with the Ombudsman, in order to remedy the infringement and mitigate the possible adverse effects of the infringement	-25% to +25%

In addition, the following may also be taken into consideration:

- The sector and size of the data controller, and the financial and other resources available to it.
- Whether the liability to pay the MPO will fall on individuals, and, if so, their status.
- The likely financial and reputational impact of the MPO on the data controller.
- Proof of any genuine financial hardship caused by the MPO.
- Any additional factors which appear to be relevant to the Ombudsman in the particular circumstances of the case in question.

Appendix 1

Breach Severity Assessment Tool – Options for Core Elements

1. TYPE OF DATA		
Select one of the types of data. If the breach covers more than one type, multiple assessments can be carried out, and the highest score should be taken as the overall severity of the breach.		
Simple data	E.g. biographical data, contact details, full name, data on education, family life, professional experience, etc.	
	Simple Data - No contextual factors	when the breach involves ’’simple data’’ and we are not aware of any aggravating factors.
	Simple Data - Possible profiling or assumptions about social / financial status	when the volume of “simple data” and/or the characteristics of the controller are such that certain profiling of the individual can be enabled or assumptions about the individual’s social/financial status can be made.
	Simple Data - Possible assumptions about health status, sexual preferences, political or religious beliefs	when the “simple data” and/or the characteristics of the controller can lead to assumptions about the individual’s health status, sexual preferences, political or religious beliefs.
	Simple Data - Critical information for personal health or safety (e.g. for vulnerable individuals, minors, etc.)	when due to certain characteristics of the individual (e.g. vulnerable groups, minors), the information can be critical for their personal safety or physical/psychological conditions.
Behavioural Data	Any type of data that is generated from an individual's actions, such as movement, preferences, etc.	
	Behavioural Data - Data provides no substantial insight into behavioural information	when the nature of the data set does not provide any substantial insight to the individual’s behavioural information or the data can be collected easily (independently from the breach) through publicly available sources (e.g. combination of information from web searches).
	Behavioural Data - No contextual factors	when the breach involves ’’behavioural data’’ and we are not aware of any aggravating or lessening factors.
	Behavioural Data - Volume of data allows for a profile of the individual and their everyday life and habits	when the volume of “behavioural data” and/or the characteristics of the controller are such that a profile of the individual can be created, exposing

		detailed information about his/her everyday life and habits.
	Behavioural Data - A profile based on sensitive personal data can be created	if a profile based on individual’s sensitive data can be created.
Financial Data	Any type of financial data (e.g. income, financial transactions, bank statements, investments, credit cards, invoices, etc.). Includes financial information relating to social welfare.	
	Financial Data - The data does not provide any substantial insight (e.g. simply identifies them as a customer)	when the nature of the data set does not provide any substantial insight to the individual’s financial information (e.g. the fact that a person is the customer of a certain bank without further details).
	Financial Data - The data includes some financial information but no significant insight (e.g. bank account numbers but no further details)	when the specific data set includes some financial information but still does not provide any significant insight to the individual’s financial status/situation (e.g. simple bank account numbers without further details).
	Financial Data - No contextual factors	when the breach involves ‘’financial data’’ and we are not aware of any aggravating or lessening factors
	Financial Data - The nature or volume of the data could enable fraud or the creation of a detailed social / financial profile)	when due to the nature and/or volume of the specific data set, full financial (e.g. credit card) information is disclosed that could enable fraud or an detailed social/financial profile is created.
Sensitive Data	E.g. health, political affiliation, religion, ethnicity, as defined in section 3 of the Data Protection Act (2021 Revision)	
	Sensitive Data - The nature of the data provides no substantial insight into behavioural information	when the nature of the data set does not provide any substantial insight to the individual’s behavioural information or the data can be collected easily (independently from the breach) through publicly available sources (e.g. combination of information from web searches).
	Sensitive Data - The nature of the data could lead to general assumptions	when nature of data can lead to general assumptions.
	Sensitive Data - The nature of the data could lead to assumptions about sensitive information	when nature of data can lead to assumptions about sensitive information.

	Sensitive Data - No contextual factors	when the breach involves ‘sensitive data’’ and we are not aware of any lessening factors.
Note: For more details, see Table 1 under Annex 1 - A1 of the ENISA Guidance, which includes worked examples for each of the data types in Annex 1 - A3 - it is important to check these examples to guide your thinking on the appropriate level to select above.		
2) EASE OF IDENTIFICATION		
Select one of the options below that describes how easy it is to identify individuals from the compromised data. The options are scored, respectively, 0.25, 0.5, 0.75 and 1. See Annex 2 of the ENISA report for worked examples of different types of data.		
The information does not permit an easy identification		
The information permits a broad identification of the individual		
The information permits a narrow identification of the individual		
The information permits identification of the concrete individual directly or through the use of public databases		
3) CIRCUMSTANCES OF BREACH		
This section takes account of the circumstances around the breach, including which type of breach it is (confidentiality, integrity or availability), along with whether there was malicious intent involved and how many data subjects have had their data compromised. In rare cases, one breach may involve more than one of these circumstances, so choose all that are relevant. See Annex 3 of the ENISA report for specific examples of how this section should be scored.		
Confidentiality breach	Loss of confidentiality and no illegal processing	
	Loss of confidentiality and known number of recipients	
	Loss of confidentiality and unknown number of recipients	
Integrity breach	Loss of integrity and no incorrect use	
	Loss of integrity and incorrect use but with possibility to recover original data	
	loss of integrity and incorrect use and no possibility to recover original data	
Availability breach	Loss of availability and easy recovery	
	Loss of availability but recovery possible with some work	
	Permanent loss of availability	
Malicious intent	Yes	
	No	
Volume of data	Fewer than 100 data subjects	
	100 or more data subjects	

SEVERITY OF DATA BREACH
This scoring matrix is taken from the ENISA report. The Calculation worksheet will automatically assign the breach to one of these categories depending on the answers to the three core sections. This score can inform our decision about the seriousness of the breach, which will feed into our investigation report.
LOW SEVERITY - Score of <1.5 - Individuals 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.)
MEDIUM SEVERITY - Score between 1.5 and 2.75 - Individuals may encounter significant inconveniences, which they will be able to overcome despite a few extra difficulties (extra costs, denial of access to business services, fear, lack of understanding, stress, minor physical ailments, etc.)
HIGH SEVERITY - Score between 3 and 4.25 - Individuals 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.)
VERY HIGH SEVERITY - Score of >= 4.5 - Individuals 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.)

Appendix 2

Matrix for Monetary Penalty Calculation

		Seriousness of Contravention			
		1 (3.0 - 3.5)	2 (3.75 - 4.25)	3 (4.5 - 5.0)	4 (5.25 +)
Degree of Culpability	None / Low	$5,000	$25,000	$45,000	$65,000
	Negligent	$25,000	$65,000	$105,000	$145,000
	Intentional	$45,000	$105,000	$165,000	$225,000

Appendix 3

References

https://ico.org.uk/media/about-the-ico/documents/2259467/regulatory-action-policy.pdf

https://ico.org.uk/media/about-the-ico/consultations/2618333/ico-draft-statutory-guidance.pdf

https://www.dataprotection.ie/sites/default/files/uploads/2019-02/Statement of Strategy 2019.pdf

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/422792/ico-guidance-money-penalties-2015.pdf

https://www.gamingtechlaw.com/2019/10/gdpr-fines-calculation.html