A regulamentação visa, justamente, orientar os agentes de tratamento quanto às suas obrigações e procedimentos de notificação. Um dos elementos centrais à decisão de notificação da autoridade é, precisamente, a existência de um incidente de segurança em "larga escala". Contudo, a redação atual não indica parâmetros para essa definição, que poderia ser melhor elaborada em um anexo que indique os critérios utilizados para considerar um incidente como "larga escala", a exemplo do que já realizou esta Autoridade com a sua metodologia da dosimetria de sanções na Resolução CD 4/2023. Pode ser definida uma metodologia que considere a (i) natureza do vazamento; (ii) natureza, sensibilidade e volume de dados pessoais; (iii) facilidade de identificação dos indivíduos; (iv) gravidade das consequências para os indivíduos; (v) características dos indivíduos; e (iv) características do controlador. Nesse sentido, a Enisa definiu metodologia (https://www.enisa.europa.eu/publications/dbn-severity) em que o grau de risco é definido a partir do contexto de tratamento em conjunto com facilidade de identificação acrescido das circunstâncias específicas do vazamento. A partir dos fatores definidos e descritos na metodologia, são determinados os níveis de risco (baixo, médio, alto ou muito alto) e as implicações decorrentes da definição do risco.

Mais informações para definição de metodologia podem ser obtidas em:

(1) Guidelines 01/2021 on Examples Regarding Data Breach Notification (https://edpb.europa.eu/sites/default/files/consultation/edpb_guidelines_202101_databreachnotificationexamples_v1_en.pdf)

(2) A Pratical Guide to Personal Data Breach Notificatiosn under GDPR (https://www.dataprotection.ie/sites/default/files/uploads/2019-10/Data%20Breach%20Notification_Practical%20Guidance_Oct19.pdf)

(3) Guidelines 9/2022 on personal data breach notification

under GDPR (https://edpb.europa.eu/system/files/2023-04/edpb_guidelines_202209_personal_data_breach_notification_v2.0_en.pdf)