GUIDELINES 01/2021 ON EXAMPLES REGARDING DATA BREACH NOTIFICATION

The International Regulatory Strategy Group (IRSG) is a practitioner-led body comprising leading UK-based representatives from the financial and professional services industry. It is an advisory body both to the City of London Corporation, and to TheCityUK. The Data workstream includes representatives from financial services firms, trade associations, the legal profession and data providers.

We welcome the opportunity to contribute the following comments, following the European Data Protection Board (EDPB) publication of guidelines on Examples regarding Data Breach Notification.

In responding, we would like to highlight the following from our Members:

1. **Overall, we welcome the new Guidance.** It is a series of practice-orientated, case-based guidance that shares Regulatory Authority experiences gained from GDPR application. It is helpful to see a Regulator approach to real-life case examples. As we continue globally to fight the pandemic, and move to vaccinations roll-outs, (which brings both new considerations for employers hoping to support their staff and work in alignment with Government programmes, and hopefully supports a safe reduction/removal of current economic restrictions), it is helpful to see pragmatic support from Regulators to apply a fair and proportionate risk-based approach to data breach assessments. The test for applying likelihood of data protection risk, should remain and not be construed/impacted by the benefit of hindsight.

2. **Context driven approach for sensitive personal data assessment:** There are areas added that provide support to organisations in helping to assess risk in data breaches. For example, Case Study 15 considers that assessment of breaches involving sensitive personal data should still remain context driven. It is helpful to see that on responsible construction, depending on the nature of the data and the breach, inclusion of sensitive personal data can still lead to an overall assessment of a breach unlikely to result in a risk to the rights and freedoms of data subjects.

3. **Security practices lists:** It is interesting to review the lists of encouraged security practices, which can be used by organisations to strengthen internal security training and reviews.

However, there are a couple of areas where refining/re-assessment would be welcomed:

Breach awareness: It would be helpful to understand that this Guidance aligns with, and is not intended to change, the position given in the 2018 Guidance, re: Regulator construction of when a controller can be considered to be "made aware" of a breach.

- This 2021 Guidance contains provision (page 6) that "*The breach should be notified when the controller is of the opinion that it is likely to result in a risk to the rights and freedoms of the data subject. Controllers should make this assessment at the time they become aware of the breach*."

- The previous Guidance contains helpful construction that Controller "awareness" of a breach should not always necessarily be when the controller is first notified of a potential incident,

but when the controller (page 11), has a reasonable degree of certainty that a data incident has occurred that has led to personal data being compromised. With the EDPB recommendation above, it would be helpful to acknowledge that there can be significant/important work to do in practice between these 2 points (from "awareness" to "notice"), which is why the GDPR provides a 72 hour period for this, extended from initial draft legislative proposals of 24 hours. And that Controllers will not be penalised or criticised by Regulators for taking the statutory allotted time to make these assessments.

Snail mail mistake. We are concerned with the drafting of the guidance in relation to Case Study 16. As drafted, the case study creates additional requirements to GDPR Article 33(1), which requires that a controller reports an incident to the competent national supervisory authority (SA) unless the incident is "unlikely to result in a risk to the rights and freedoms of natural persons" and creates an obligation on a controller to assess the factual matrix of an incident and give reasoned consideration to any actual risk to the rights and freedoms of the data subject. We believe that this is the true test of whether an incident should be reported to a SA and that decision can only be made following such an assessment.

- We would therefore conclude that the guidance should be amended to say that where a piece of correspondence containing limited personal data of an individual has been inadvertently included within correspondence to another individual, this should not be classed as a reportable incident to the SA, unless the controller, having conducted an assessment of the factual matrix, determines that there is a real risk to the rights and freedoms of the data subject.

Commercial delays qualify as a risk to data protection rights and freedoms. One curious assessment is at Case Study 2, which provides an example of a ransomware attack, with an online back-up failure, which the controller is able to mitigate with existing paper back-ups. The assessment identifies no personal data 'data' gaps or losses; only that within a week the controller has been able to take steps to mitigate, and this leads to the consequence of "minor delays in order delivery" and loss of meta-data (e.g. logs, time-stamps).

- It is not clear how the link is made between a "minor order delay" being construed to result in data protection risk. If the example is understood correctly, the "damage to reputation" here would be to the Controller's reputation (in not fulfilling expectations on delivery timescales), not to the data subject reputation as a result of compromised data (as in this example this is encrypted data, not exfiltrated and confidentiality of the personal data "is not compromised" (page 9)).

Extent of Regulator involvement in the form of data breach communications: Case Study 5, considers that where a breach is high risk, this means (page 15) that "of course … that the relevant SA(s) should also be involved in the form of a data breach notification." It is acknowledged that controllers should, in this situation, work in close co-operation with the relevant regulatory authority, and respect the guidance it provides; but GDPR at Article 34(1), and in line with accountability principles, places the obligation solely with the controller to be responsible for communicating a personal data breach to impacted data subjects, without delay.

Language. We feel that there is an inconsistent use of the term "financial data" in the Guidelines which needs to be made clearer in order for the market to understand why a breach of financial data is particularly severe. Language also needs to be further refined as currently the examples assume that any data which is at rest can be encrypted, which is not always possible or advisable. We would also suggest adding a reference in the Guidelines to industry accepted security standards for preventing/mitigating different types of attacks such as the NIST Cybersecurity Frameworks.

For any questions or clarifications please contact: IRSGsecretariat@cityoflondon.gov.uk.

ANNEX – IRSG DATA WORKSTREAM MEMBERSHIP

- London Stock Exchange Group
- ABI
- AFME
- AIMA
- Bank of America
- Barclays
- BNY Mellon
- CBI
- Citi
- Clifford Chance
- Credit Suisse
- DLA Piper
- Fidelity
- FLA
- Freshfields
- HSBC
- IA
- Invesco
- IBM
- JP Morgan
- Lloyds Banking Group
- Marsh UK & Ireland
- Mastercard
- Morgan Stanley
- Nasdaq
- PIMFA
- Standard Chartered
- techUK
- UK Finance