European Federation of Pharmaceutical Industries and Associations

EFPIA Response to EDPB consultation on Guidelines 01/2021 on Examples regarding Data Breach Notification

EFPIA welcomes the opportunity to comment on the draft Guideline, which is a comprehensive and useful document. It is particularly useful to have the extensive list of scenarios provided in the Guideline. We would like to suggest that the final Guideline would be enhanced by the inclusion of further case studies relating to pseudonymized or de-identified data. The use of such data is common in clinical trials and scientific research involving health data. In these cases, data is held in a form which may still be considered to be within scope of GDPR (i.e. pseudonymised data), but in which the data holder either cannot directly identify the individual through reasonable means or can only do so through cooperation with a third party holding the code key.

As a result, there may be, at a minimum, at least two organisations involved in addressing the breach. The coding is normally carried out by a health care professional within a healthcare institution/organisation in order to comply with confidentiality and data minimization principles consistent with the purpose of the processing and is intended to protect the individual. Sensitive data would invariably be implicated in the breach (e.g. health data, genetic information and sometimes sex life). A breach may occur within the health institution which holds fully identifiable data, or in the systems owned or controlled by the clinical trial Sponsor, which would typically only store pseudonymised trial participant data, plus clinical staff contact details and qualifications. There is a need for alignment between the relevant controllers regarding the assessment of a breach and the responsibilities of the parties. In addition, any disclosure to the Sponsor of the clinical trial of the identity of the subjects participating in the clinical trial for the purposes of responding to breach notification obligations may raise unrelated legal and regulatory issues, as the Sponsor is not meant to know the identity of the subjects participating in clinical trials. We would welcome insertion of a case study related to this scenario, which can provide better clarity of the responsibilities of the parties regarding breach investigation, tracking and reporting obligations, as well as clarify if breaches involving pseudonymous data require notification or if this is only the case if fully identifiable data was compromised.

A further example from the health research sector, also raising the question of coordination between controllers, involves a breach of clinical trial data submitted to public authorities as part of a regulatory or legal requirement (e.g. clinical trial data submitted to the European Medicines Agency – EMA – for drug market authorisation purposes in the EU) . Such regulatory submissions will contain a mixture of identifiable data (e.g. contact details and credentials from investigators and Sponsor staff responsible for the trial) and coded/pseudonymised data (from trial participants, such as gender, age, date of birth, health data, lab results, genetic analysis, etc). The same issues of coordination among controllers arise in the case of a breach that takes place at the authority (e.g. EMA), which is necessarily an independent controller of the data.

EFPIA suggests that the Guideline would be further strengthened by examples of this sort. EFPIA members have extensive knowledge of these situations which they are keen to share. We would welcome dialogue with the Board, which we believe could further improve the Board's draft document.