REMEDIATION AND REPORTING OF PERSONAL DATA BREACH

GSK required to report any Personal Data Breach where there is a risk to the rights and freedoms of the Data Subject.

1. Where the Personal Data Breach results in a high risk to the Data Subject, he/she also has to be notified **72 hours** from the time of the breach or as soon as possible unless subsequent steps have been taken to ensure that the risk is unlikely to materialise, security measures were applied to render the Personal Data unintelligible (e.g. encryption) or it would amount to disproportionate effort to inform the Data Subject directly. In the latter circumstances, a public communication must be made, or an equally effective alternative measure must be adopted to inform Data Subjects, so that they themselves can take any remedial action.

2. GSK have put in place procedures to deal with any suspected Personal Data Breach and will notify Data Subjects or the relevant regulator where GSK are legally required to do so. All suspected breach of Personal Data should be remedied with 1 (one) month from the date of the report of the breach.

3. If you know or suspect that a Personal Data Breach has occurred, you should immediately contact the Data Protection Officer – Frederick.e.ichekwai@gsk.com GSK will retain all evidence relating to Personal Data Breaches in particular to enable GSK to maintain a record of such breaches, as required by the Data Protection Laws.

4. Records of Personal Data Breaches must be kept by each employee or member of staff who observes or has reason to believe that a Data Breach has occurred. The record must set out:
    a. the facts surrounding the breach;
    b. its effects; and
    c. the remedial action taken.

5. GSK will not be responsible for any Personal Data breach which occurs as a result of:
    a. an event which is beyond the control of GSK;
    b. an act or threats of terrorism;
    c. an act of God (such as, but not limited to fires, explosions, earthquakes, drought, tidal waves and floods) which compromises GSK's data protection measures;
    d. war, hostilities (whether war be declared or not), invasion, act of foreign enemies, mobilisation, requisition, or embargo; and
    e. rebellion, revolution, insurrection, or military or usurped power, or civil war which compromises GSK's data protection measures;
    f. the transfer of your personal data to a third party on your instructions; and
    g. the use of your personal data by a third party designated by you.