APPROVED:
Engineer Vladimir Spasov
Procurator

Internal procedure for notification in case of personal data security breach at "M+S Hydraulic" PLC.

This procedure is to be applied in the cases of personal data security breach as per article 33 and article 34 of the General Data Protection Regulation (EU) 2016/679 ("GDPR").

A breach of data security arises when the personal data, for which "M+S Hydraulic" PLC. is responsible, is affected by security incident as a result of which personal data confidentiality, availability and integrity are broken. In this sense, a breach of personal data occurs when there is a security breach leading to accidental or unlawful destruction, loss, alteration, unregulated disclosure of data which is transferred, stored or processed in another way.

The procedure is also applied under the instruction of the Commission for Personal Data Protection under the circumstances, occurring in the cases of a breakthrough in spite of the technological measures which the company has undertaken in order to protect the security of the personal data, subject of this breach.

1. After the respective employee of "M+S Hydraulic" PLC., in their capacity of an official, dealing with the personal data processing under the guidance of the Administrator, gets suspicious of a breach of the security of personal data, they are to inform **the Person responsible for personal data protection** who is to decide whether the particular event is a case of personal data breach and to inform the procurator about the event.
2. In case of personal data security breach, which is likely to put at risk the rights and liberties of physical persons, the Administrator (through **the Person responsible for personal data protection**), without unnecessary delay and whenever this is realizable – no later than 72 hours after this has come to their knowledge, is to notify the Commission for Personal Data Protection about the breach.

The notification should include at least the following:

a) Description of the nature of the personal data security breach including, if possible, the categories and the approximate number of data subjects affected, as well as the categories and the approximate quantity of the personal data records affected;
b) Indicating the name and contact information of the data protection official or of another contact point from which more information could be obtained;
c) Describing the possible consequences of the personal data security breach;
d) Describing the measures undertaken or offered by the administrator for coping with the personal data security breach, including, where appropriate, measures for reducing the possible unfavourable consequences.

3. When and as far as it is not possible for the information to be submitted simultaneously, the information is to be submitted stage-by-stage without further unnecessary delay.

4. The notification to the supervisory body is to include the reasons for the delay in the cases it has not been submitted within 72 hours.

5. In case the personal data security breach is likely to put at high risk the rights and liberties of physical persons, the Administrator, through **the Person responsible for personal data protection** and without unnecessary delay, is to inform the data subject about the personal data security breach.
6. The notification to the data subject is to include at least the following information:
    a) Description of the nature of the personal data security breach;
    b) Indicating the name and contact information of the data protection official or of another contact point from which more information could be obtained;
    c) Describing the possible consequences of the personal data security breach;
    d) Describing the measures undertaken or offered by the administrator for coping with the personal data security breach, including, where appropriate, measures for reducing the possible unfavourable consequences.
7. The Administrator is to inform every physical person about the occurrence of a breach of the personal data security in an easily comprehensible form using plain and clear language.
8. There is no message to the data subject required if:
    a) The Administrator has undertaken appropriate technical and organizational protection measures and these measures have been applied with regard to personal data, affected by the personal data security breach, in particular the measures which render the personal data incomprehensible for every person who does not have the permission to access it;
    b) The Administrator has subsequently undertaken measures guaranteeing no more chances of materialization of the high risk for the rights and the liberties of data subjects;
    c) This would result in disproportionate efforts. In such a case, a public announcement is to be made or a similar measure is to be undertaken, so that the data subjects would be informed with equal effectiveness.
9. The personal data Administrator, through **the Person responsible for personal data protection** is to document each personal data security breach, including the facts, related to the personal data security breach, the consequences from it and the actions undertaken in order to cope with it. This documentation makes it possible for the supervisory body to check if article 33 of the General Data Protection Regulation has been observed.

This procedure has been ratified by the Procurator on **25.05.2018** by virtue of Order № 248/25.05.2018 and is to be supplemented and amended in the order of its ratification.