Personal Data Protection Policy

pursuant to Article 24 of the GDPR

Foundation for MultiMedia Communications
London Representative Office

last update on 24 July 2018

0. Definitions

Organization	means Foundation for MultiMedia Communications(FMMC), London Representative Office.
GDPR	means the General Data Protection Regulation.
Responsible Person	means Director of the FMMC London Office.

1. Data protection principles

The Organization is committed to processing personal data in accordance with its responsibilities under the GDPR.

Article 5 of the GDPR requires that personal data shall be:

a. processed lawfully, fairly and in a transparent manner in relation to individuals;
b. collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;
c. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
d. accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
e. kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and
f. processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.”

2. General provisions

a. This policy applies to all personal data processed by the Organization.
b. The Responsible Person shall take responsibility for the Organization's ongoing compliance with this policy.
c. This policy shall be reviewed at least annually.

3. Lawful, fair and transparent processing

a. To ensure its processing of personal data is fair and transparent, the Organization shall provide individuals with relevant information on why and how it processes their personal data pursuant to Article 13 or 14 of the GDPR.
b. Individuals have the right to access, rectification, erasure, restriction of processing, data portability, object to processing and not being subject to fully automated decision-making concerning their personal data pursuant to Chapter 3 of the GDPR.
c. Any such requests or claims made to the Organization shall be dealt with in a timely manner, usually within one month of receit of such requests or claims.

4. Lawful purposes

a. All processings of personal data by the Organization must be done on one of the following lawful bases: consent, contract, legal obligation, vital interests, public task or legitimate interests.
b. The Organization shall identify the appropriate lawful basis.
c. Where consent is relied upon as a lawful basis for processing personal data, evidence of opt-in consent shall be kept with the personal data.
d. Where communications are sent to individuals based on their consent, the option for the individual to revoke their consent should be clearly available and procedures should be in place to ensure such revocation is reflected accurately in the Organization's systems.

5. Data minimisation

a. The Organization shall ensure that personal data are adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
b. The Responsible Person shall review, at least annually, the personal data collected is limited to what is really necessary in relation to the purposes for which they are processed.

6. Accuracy

a. The Organization shall take reasonable steps to ensure personal data is accurate.
b. Where necessary for the lawful basis on which personal data is processed, steps shall be put in place to ensure that personal data is kept up to date.

7. Archiving / removal

a. To ensure that personal data is kept for no longer than necessary, the Organization shall put in place an archiving or removal policy for each area in which personal data is processed and review this process annually.
b. The archiving or removal policy shall consider what personal data should/must be retained, for how long, and why in accordance with the information provided to the relevant individuals.

8. Disclosure

When the organization needs to disclose personal data to any third-party entity for the purpose of the processing, it shall provide the individuals with the information on such disclosure at the time when it collects personal data or it shall obtain consent of the individuals to do so. Without such information or consent, the Organization shall not disclose personal data to any third-party entitiy unless it is required to disclose personal data to competent public authorities under legal obligations it is subject to.

9. Third-Country Transfer

When the organization needs to transfer personal data to any third-country outside of the European Economic Area, it shall ensure that appropiate safegurard is in place or any exemption applies pursuant to Chapter 5 of the GDPR.

10. Security

a. The Organization shall ensure that personal data is stored securely using modern software that is kept-up-to-date.
b. Access to personal data shall be limited to personnel who need access and appropriate security should be in place to avoid unauthorised sharing of information.
c. When personal data is deleted this should be done safely such that the data is irrecoverable.
d. Appropriate back-up and disaster recovery solutions shall be in place.
e. The Responsible Person shall review such security measures at least annually. Such annual review shall be done in the following way:
    i. assessing the risk caused by each processing by identifying the source of risks (e.g. person, system, operation procedure) and evaluating the likelihood and severity of possible consequences caused by each risk;
    ii. determining measures to deal with each risk (e.g. controlling access to system/premises, backups, traceability, encryption, pseudonymization, etc.); and
    iii. implement and enforce such measures.
f. The Responsible Person shall specify particular security measures for each processing.

11. Breach Notification

In the event of a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data, the Organization shall promptly assess the risk to people’s rights and freedoms and if appropriate report this breach to the Information Commisioner’s Office.