March 2018

The Interpublic Group of Companies, Inc.

Client Pack

IPG Agencies GDPR Security Technical and Organisational Measures

---

1. Physical access control

Technical and organisational measures to prevent unauthorized persons from gaining access to the data processing systems available in premises and facilities (including databases, application servers and related hardware) where Personal Data are processed, include: Establishing security areas, restriction of access paths;

- Establishing access authorisations for employees and third parties;
- Access control system (ID reader, magnetic card, chip card);
- Key management, card-keys procedures;
- Door locking (electric door openers etc.);
- Security staff, janitors;
- Surveillance facilities, video/CCTV monitor, alarm system;
- Securing decentralised data processing equipment and personal computers.

2. Virtual access control

Technical and organisational measures to prevent data processing systems from being used by unauthorised persons include:

- User identification and authentication procedures;
- ID/password security procedures (special characters, minimum length, change of password);
- Automatic blocking (e.g. password or timeout);
- Monitoring of break-in-attempts and automatic turn-off of the user ID upon several erroneous passwords attempts;
- Creation of one master record per user, user master data procedures, per data processing environment;
- Encryption of archived data media.

3. Data access control

Technical and organisational measures to ensure that persons entitled to use a data processing system gain access only to such Personal Data in accordance with their access rights, and that Personal Data cannot be read, copied, modified or deleted without authorisation, include:

- Internal policies and procedures;
- Control authorisation schemes;
- Differentiated access rights (profiles, roles, transactions and objects);
- Monitoring and logging of accesses;
- Disciplinary action against employees who access Personal Data without authorisation;
- Reports of access;
- Access procedure;
- Change procedure;
- Deletion procedure;
- Encryption.

4. Disclosure control

Technical and organisational measures to ensure that Personal Data cannot be read, copied, modified or deleted without authorisation during electronic transmission, transport or storage on storage media (manual or electronic), and that it can be verified to which companies or other legal entities Personal Data are disclosed, include:

- Encryption/tunnelling;
- Logging;
- Transport security.

5. Control of instructions

Technical and organisational measures to ensure that Personal Data are processed solely in accordance with the Instructions of the Controller include:

- Unambiguous wording of the contract;
- Formal commissioning (request form or Statement of Work);
- Criteria for selecting any Sub-Processor.

6. Availability control

Technical and organisational measures to ensure that Personal Data are protected against accidental destruction or loss (physical/logical) include:

- Backup procedures;
- Mirroring of hard disks (e.g. RAID technology);
- Uninterruptible power supply (UPS);
- Remote storage;
- Anti-virus/firewall systems;
- Disaster recovery plan.

7. Separation control

Technical and organisational measures to ensure that Personal Data collected for different purposes can be processed separately include:

- Separation of databases;
- “Internal client” concept / limitation of use;
- Segregation of functions (production/testing);
- Procedures for storage, amendment, deletion, transmission of data for different purposes.