August 2018

The Interpublic Group of Companies, Inc.

IPG’s GDPR Vendor Pack

Requirements for Processing Personal Data where a Vendor is acting as a Controller and/or a Processor on behalf of IPG

Data controllers and processors each have obligations under the General Data Protection Regulation (GDPR).

IPG has produced this document to set out what is **required from all Vendors if**:

- the **services** provided by a Vendor involve the **processing of personal data** that are covered by **the GDPR**,
- those services are for **the benefit of IPG and/or its clients**, and
- the **Vendor** is acting as a **controller, processor or sub-processor**.

In this document:

- IPG, “We” or “Us” shall mean IPG, its agencies and/or subsidiaries, and
- “Services” shall be construed as outlined above.

SECTION I:

IPG’s Requirements where a Vendor Processes Personal Data covered by the GDPR as a Data Processor when providing Services

Where a Vendor processes personal data as a data processor as part of any Services, that Vendor **must**:

- have appropriate security measures in place at all times when handling personal data;
- comply at all times with the requirements set out in **Section III: *Security, Technical and Organisational Measures IPG Vendors Must Adopt***;
- ensure their employees fully understand and maintain the confidentiality of all personal data;
- ensure only authorised personnel are permitted to handle personal data on IPG’s behalf;
- not transfer or share the personal data provided to them for the performance of the Services with any third party without advising IPG of that intention first and obtaining IPG’s prior consent;

- only process personal data in accordance with IPG's instructions - including deletion - and in accordance with the law;
- not transfer any personal data provided for the Services outside the EEA without first advising IPG of that intention and obtaining IPG's prior consent;
- respond promptly to all requests for changes to be made to any personal data;
- notify IPG within 24 hours of any breach;
- keep IPG promptly and fully informed of each and any incident involving personal data;
- respond reasonably to audit requests;
- where a Vendor is required by the GDPR to have a Data Protection Officer (DPO), provide details of their DPO, including comprehensive contact details; and
- always
    - maintain up-to-date summaries of the following, as carried out by the Vendor:
        - the security, technical and organisational measures applied to personal data,
        - all compliance, governance and training activities, and
        - the data processing operations carried out as part of the Services; and
    - make copies of these summaries available on request to ensure IPG is always aware of processing practices and can keep track of processing activities accurately at any time.

Where IPG:

- is a data controller, in respect of the Services, IPG will agree detailed services before any Services begin – and identify any data processing to be undertaken by a Vendor.
- is a data processor, acting on behalf of an IPG client or other third party, and a Vendor is acting as a sub-processor, IPG shall ensure that processing instructions are obtained from the relevant data controller and that relevant processing instructions are communicated to the Vendor.

If a Vendor thinks there is an issue with any instruction at any time, the Vendor must let IPG know and not process any personal data until this issue has been resolved.

SECTION II:

IPG's Requirements where a Vendor Processes or Provides Personal Data covered by the GDPR as a Controller when providing Services

In all cases where a Vendor processes or provides personal data as a data controller as part of any Services that

Vendor **must:**

- establish a lawful basis for processing or providing that personal data under the GDPR prior to providing any Services - whether this is through consent, legitimate interests, performance of a contract, or otherwise;

- provide IPG with clear instructions on any limitations on use that may apply to the personal data, for example, any retention periods;

- ensure that any personal data provided to an IPG entity can be shared with other IPG entities – and if, this is not permitted for any reason, make this known to IPG prior to any processing;

- only process and/or provide data that is necessary for the performance of the Services, and

- comply with the requirements and principles set out in Section I.

As a global network with operations in a number of EU countries and beyond, operationally, IPG often shares or transfers personal data within the IPG group.

Where IPG is acting as a processor of personal data for which a Vendor is the controller, IPG will consult that Vendor before appointing an external processor/sub-processor outside of IPG.

SECTION III:

Security, Technical and Organisational Measures IPG's Vendors Must Adopt

Whether acting as either a controller or processor, all Vendors providing services to IPG must have appropriate security measures in place at all times when handling personal data as part of the Services. As a minimum, these security, technical and organisational measures should include the following at all times:

Technical and Organisational Measures:

a. Physical Access Controls

To prevent unauthorised 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, to 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.

b. Virtual Access Controls

To prevent data processing systems from being used by unauthorised persons, to 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.

c. Data Access Controls

To ensure that persons entitled to use a data processing system gain access only to personal data in accordance with their access rights, and that personal data cannot be read, copied, modified or deleted without authorisation, to 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.

d. Disclosure Controls

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, to include:

- encryption/tunnelling;
- logging;
- transport security.

e. Control of Instructions

To ensure that personal data are processed solely in accordance with our instructions.

f. Availability Controls

To ensure that personal data are protected against accidental destruction or loss (physical/logical), to include:

- backup procedures;
- mirroring of hard disks (e.g. RAID technology);
- uninterruptible power supply (UPS);
- remote storage;
- anti-virus/firewall systems;
- disaster recovery plan.

g. Separation Controls

To ensure that personal data collected for different purposes can be processed separately, to 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.