December 2018

The Interpublic Group of Companies, Inc.

The way IPG Agencies will handle personal data for our clients

Our clients, as data controllers, and our agency, as their appointed data processor, have obligations under the General Data Protection Regulation (GDPR). We have produced this document to explain to you, as our client, how we handle personal data on your behalf and to ensure you understand our approach. It sets out useful information to support your compliance with the GDPR as a controller and explains how we will support you as your appointed processor.

Security Measures, Confidentiality and Compliance

We will make sure that:

- we have appropriate security measures in place when handling personal data; and
- our employees fully understand and maintain the confidentiality of that personal data - only authorised account handlers will be permitted to handle each client's personal data.

We will always maintain up to date summaries of:

1. the security measures we apply to personal data;
2. our GDPR compliance, governance and training activities; and
3. key features of the data processing operations our agency carries out for clients.

We will provide these summaries to you when we are engaged to process personal data for you for the first time and periodically thereafter so that you are always aware of our practices. These summaries are called:

1. **"Our GDPR Security Technical Measures",**
2. **"What we are doing to comply with the GDPR" and**
3. **"Our Data Processing Operations – Key Features".**

Your Instructions

We typically agree detailed services for clients before our services begin – usually in a statement of work (SOW) – and identify any data processing to be undertaken. We will only use personal data as instructed by you and in accordance with the law. If we think there is an issue with any instruction at any time, we will let you know.

What we will expect of you

As the data controller, where you provide us with the personal data of EU residents we will require you to have established that there are lawful grounds for us to process the data before you provide it to us. In addition, where you are asking us to engage with individuals on your behalf and acquire their data for your marketing or other purposes, we require you to provide any privacy notice or policy used to obtain any necessary consents from those individuals. Our agencies cannot know all your long term aims, so, at the same time as being a legal obligation imposed on you as a data controller, this also makes good commercial sense.

Consent

Transparency is key when obtaining consent to use personal data. To achieve this, we understand that it is necessary to provide individuals with clear and unambiguous explanations of the potential use of the data so that the consent obtained is informed consent. To help with this we will provide appropriate use cases and summaries of data usage so that you - or any other data collectors - will have the knowledge and understanding needed to fully and clearly explain potential data usage to individuals at the time of obtaining consent and also to help assess whether any consent already obtained can be used for the intended project.

Where we broker the use of personal data on your behalf – for example for online targeted ad-serving - we will seek assurances from the data provider that you can use that data lawfully for your purposes (through consent or otherwise) – even though we are unlikely to receive the personal data ourselves or process it in any way. We will also endeavour to provide explanations of how they operate so that you are clear on what and how data may be used and you can include any relevant details in your privacy notices and policies.

Sub-processing

Sub-processing within our Agency Network: We may sometimes ask that you consent to us sharing or transferring personal data to other agencies in our group. We are part of a global network that has operations in a number of EU countries and beyond. To help us provide the best service to you we sometimes need to work closely with other companies in our group. All companies in our group are expected to handle personal data to the same standards so we can give you peace of mind that any personal data used within our group is being processed in accordance with your instructions and all relevant laws, including the GDPR.

Outside our Agency Network: Outside our group, we will routinely obtain your consent before appointing an external sub-processor – save as set out below.

Media Services: A significant area where pre-notification of all sub-processors is difficult – if not impossible - is for certain online advertising/media services. This is because - for these services - sub-processors are appointed following a successful real-time bid for advertising space on a publisher's website and the advertisement is then published immediately after that successful bid. Given the split-second speed of this process and, obviously, being unable to predict the outcome of the bidding process, it is impossible for clients to be given advance notice of the identity of the ultimate publishers and data processors and, therefore, the right of pre-approval. So, where

advance identification of processors or sub-processors is problematic, we will endeavour to provide clear explanations of how such services operate. In this way, you, as the data controller, can fully understand what and how personal data may be acquired or used by sub-processors when we are delivering those services.

Processors/Sub-processors with Non-Negotiable Terms: Some third party processors/sub-processors will only provide their services under non-negotiable contractual terms – we call these third parties Fixed Term Vendors or FTVs. And often these FTVs are critical to the provision of certain advertising services, for example, Google and Facebook for online advertising/media services. Where an FTV is to be appointed, we will provide you with their details and assist you in ascertaining their contractual terms. Unless you object, their appointment and terms of business will be deemed approved and accepted by you, and our liability and obligations will be limited to and not exceed those of the FTV in respect of the data processing carried out by them for you.

Transfers outside the EEA

We will not transfer personal data to any third party who we believe will either use or transfer that data outside of the EEA unless an adequate level of protection is provided through Privacy Shield, EU Model Clauses or an equivalent mechanism. We will pass on this requirement, and all other compliance requirements, to any sub-processors we may appoint to provide services to you.

Our DPO

You can always find details of the DPO appointed to act on our behalf in relation to the GDPR in our document: **"What we are doing to comply with the GDPR".**

Your obligations and our help

As a controller, you have a range of obligations including: to respond to data subjects' requests; adhering to strict reporting requirements in the highly unfortunate event of a data breach; establishing when a data processing impact assessment (DPIA) is needed, and carrying out DPIAs.

We, as your processors, are committed to assisting you: we will respond to all requests for changes; react promptly and professionally to any breach to keep you fully informed; provide information about the way we process data for you; and respond to audit requests.

In relation to requests from individuals, we hope to significantly reduce the need for us to make changes to personal data through our ways of working. For each project we will ensure the accuracy of the data by only using the up to date personal data provided by you or acquired on your behalf, and then deleting that data once the project has ended and there is no justification for us to keep it. If requested, we will provide you with a copy of that personal data prior to deletion.