04. Data Privacy

▶ AT A GLANCE

- Data privacy compliance is vital to our business and that of our clients. We are **committed to the responsible use and safeguarding** of sensitive and personal information.
- We have developed a global data privacy program run by the Global Data Privacy Office (GDPO) to ensure we **comply with applicable data privacy laws.**
- We respect privacy rights and are dedicated to ensuring that sensitive and personal information is handled in strict accordance with the law.

FOR WHOM?

All employees as well as contractors, vendors and subcontractors.

WHAT?

- Groupe data privacy policies have been developed to ensure that:
  - personal Information is collected and used in accordance with applicable data privacy laws;
  - the personal information the Groupe holds on behalf of clients is properly protected so that the Groupe can help clients comply with their own legal obligations;
  - requests from individuals for access to their own personal information are adequately managed;
  - requests from third parties for access to personal information are adequately managed.
- Employees are required to complete regular data privacy trainings from the moment they join Publicis.

HOW?

Global Data Privacy Program

- The Groupe has established a global data privacy program run by the Global Data Privacy Office (GDPO).
- This aims to ensure that the Groupe collects and uses Personal Information in accordance with applicable data privacy laws such as the General Data Protection Regulation (GDPR).

Personal Information

- Personal Information may include information about employees, clients, prospects, suppliers and other business contacts.
- It may also include consumer-related information collected by the Groupe, or obtained from clients or third-party providers.
- Examples of Personal Information are names, addresses, phone numbers, social security numbers or a user's IP address, pseudonymous identifiers, and behavioral attributes.

Sensitive Personal Information

- Sensitive Personal Information often includes information that relates to an individual's health, sexual, racial, or religious status, trade union membership or political affiliations.
- As a general rule, the Groupe should not need to collect and use such Sensitive Personal Information for its legitimate business activities.
- The collection and use of such information or the provision of such information by any supplier or client needs the prior approval of the Groupe Chief Data Privacy Officer.
- Any Sensitive Personal Information obtained by any means must be treated with the highest degree of protection in accordance with the law and internal policies and procedures.

Using Personal Information

- All Business Units in Countries must ensure that any use of Personal Information is lawful and in accordance with the Publicis Groupe global data privacy program. All employees, contractors, vendors, and subcontractors dealing with Personal Information must be aware of the strict laws and regulations applying to the collection, use, storage, and processing of such Personal Information.

Compliance with such laws and regulations is mandatory.

- Contracts with clients and vendors must address legal and business issues related to Personal Information. This includes placing appropriate restrictions on the collection, treatment and use of data, applying confidentiality requirements, and identifying the rights and restrictions associated with information in accordance with Groupe data privacy policies.
- The IT department in each region is responsible for ensuring that current systems and infrastructure are sufficient to secure data and all sensitive and/or personal information.
- All Business Units in the Countries must put in place procedures and protocols for handling any unauthorized disclosure.

  This must be done in accordance with the data privacy policies, procedures and tools developed by the GDPO as well as the security policies, procedures and guidance from the Global Security Office.

REACHING OUT TO THE GLOBAL DATA PRIVACY OFFICE

- The Groupe Chief Data Privacy Officer must be promptly informed of any:
  - formal inquiry from a data protection authority;
  - request from an individual for access to their Personal Information; or
  - unauthorized disclosure of information to third parties in line with relevant policies and procedures.
- As the laws and regulations vary according to jurisdiction, where there is any doubt, Business Units must seek advice from the Global Data Privacy Office (GDPO).

WHO?

Business Unit and Country CEOs and CFOs and the Groupe Chief Data Privacy Officer.

Policy available to the public on the Groupe website.