

GLOBAL DATA PRIVACY POLICY SUMMARY

APPLICABILITY AND SCOPE

Publicis Groupe (“**Publicis**”, “**we**”, or “**us**”) are committed to providing a high level of privacy and security of Personal Data. “**Personal Data**” is any information about an identifiable person. A person can be identified by their name, device ID, address, or many other data points. The concept of Personal Data has evolved beyond “Personally Identifiable Information” or “PII”, a term used for many years prior to the passage of new data privacy laws like the General Data Protection Regulation (GDPR) and US state laws.

Publicis has adopted the following restricted and non-public facing policies (“**Policies**”) that apply to the processing of Personal Data by Publicis globally.

Publicis Data Privacy Policies	Status
(1) Global Data Privacy Policy	Restricted
(2) Data Handling Policy	Restricted
(3) Public Authority Request Policy	Restricted
(4) Risk Assessment & Mitigation Policy	Restricted
(5) Individual Request Policy	Restricted
(6) Privacy by Design & Privacy by Default Policy	Restricted
(7) Publicis Data Privacy Policies Summary	Public

All employees, contractors, consultants, freelancers, and other members of the Publicis workforce (“**Publicis Personnel**”) are obligated to adhere to these Policies.

This Global Data Privacy Policy Summary is intended to provide an outline of the set of rules for the management and use of Personal Data presented in the above Policies.

FAQ

WHAT IS DATA PRIVACY LAW?

In many jurisdictions the right to a private life and associated freedoms are considered fundamental human rights, and it is this basic concept that is the rationale behind data privacy law. Data privacy law governs the collection and use of Personal Data and provides individuals with rights to control and understand how their Personal Data is being used. It also places obligations on organizations such as Publicis that use Personal Data.

Data privacy law is usually enforced by data protection authorities (e.g., UK ICO and French CNIL) as well as the relevant courts.

HOW DOES DATA PRIVACY LAW AFFECT PUBLICIS GROUPE?

Agencies within Publicis all hold and use Personal Data in various capacities. The use of Personal Data is often a key component of the products and services we provide to clients.

WHAT ARE WE DOING ABOUT IT?

Publicis takes compliance with data privacy law very seriously. We wish to maintain the highest possible standards and ensure that Publicis Personnel are properly trained, and that our internal procedures are designed for compliance. We have developed these Policies to demonstrate our commitment to data privacy compliance and to show that we have processes and protocols in place designed to protect individual's privacy and address compliance. These policies are regularly reviewed.

ARE WE A DATA PROCESSOR OR A DATA CONTROLLER?

Publicis is a large organization with many different product and service offerings. Therefore, each agency may be acting as a Controller or a Processor, in each case depending on the particular product or service provided and the specific circumstances.

A “**Controller**” determines the purpose for collecting, storing, destroying, analyzing, or otherwise using (collectively, “**processing**”) Personal Data. Under data privacy law in certain jurisdictions, Controllers may be referred to by a different term such as a **Businesses, Organizations, or Third Parties**.

A “**Processor**” processes Personal Data in accordance with a Controller’s instructions and only for those purposes. For example, if our client sends us its customer file and instructs us to send direct mail to the Individuals on the list and not to use it for any other purpose, we are a Processor. Under data privacy law in certain jurisdictions, Processors may be referred to by a different term such as **Service Providers** or **Contractors**.

WANT MORE INFORMATION?

If you want more information about how Publicis process Personal Data, please reach out to your local contact at the applicable Publicis agency.

SUMMARY OF THE POLICIES

PUBLICIS GLOBAL DATA PRIVACY POLICY

This Policy provides the core data privacy principles all Public Personnel need to adhere to. Such principles include:

- Lawfulness, fairness and transparency;
- Honoring individual’s rights;
- Purpose limitation;
- Data minimization;
- Accuracy;
- Storage limitation;
- Integrity and confidentiality;
- Risk analysis and mitigation;
- Vendor management;
- Sharing Personal Data;
- Ensuring adequate protection for international transfers; and
- Processing sensitive Personal Data

DATA HANDLING POLICY

This Policy provides a global baseline across Publicis of guidelines for the handling of Personal Data from clients, vendors and consumers and includes practical steps of data handling in accordance with the principles listed above. For example, it requires all Publicis Personnel to (i) ensure pseudonymization and encryption where possible; (ii) conduct assessments prior to data onboarding; (iii) implement data retention plans; and (iv) conduct data privacy training.

PUBLIC AUTHORITY REQUEST POLICY

This Policy sets out Publicis processes concerning: (i) requests to disclose Personal Data from or enforced by a public authority, such as law enforcement, a government agency or regulator, or a court of law, and (ii) any court order requesting the same; issued by a competent jurisdiction to benefit surveillance or law enforcement agencies, or any other government agency in charge of enforcing or maintaining legal order in a country. Generally, any requests to retain or disclose Personal Data made to Publicis must be:

- Under a valid court order, subpoena, warrant, writ, decree, summons, or other legally binding order, for instance, valid orders to search, disclose or inspect any premise occupied by or material in possession of Publicis; or
- Made to cover proven emergency circumstances (such as to prevent imminent danger of death or serious injury), to the extent that applicable legal provisions permit this.

Generally, Publicis shall never disclose Personal Data in a massive, disproportionate, and indiscriminate manner that goes beyond what is necessary in a democratic society.

RISK ASSESSMENT AND MITIGATION POLICY

This Policy provides Publicis Personnel with guidelines on how to conduct Privacy Impact Assessments and Data Protection Impact Assessments and where such are necessary or desirable, with the intention of identifying and mitigating risks to individuals.

INDIVIDUAL REQUEST POLICY

This Policy provides guidelines for managing and responding to lawful requests made by individuals under data privacy laws, such as GDPR and US state laws including:

- the right to **access** Personal Data
- the right to **erase** Personal Data
- the right to **object/opt-out** of processing of Personal Data

Other rights, include:

- the right to **rectify** or **correct** any incorrect Personal Data
- the right to **restrict** the processing of Personal Data
- the right to data **portability**
- the right to **not to be subject to automated decision making** which has a legal effect or similar significant effect on the Individual.
- the right to **opt-out of the sale/share** of Personal Data

PRIVACY BY DESIGN AND DEFAULT POLICY

This Policy guides Publicis Personnel on how and when to integrate data protection considerations into our processing activities and how to implement appropriate technical and organizational measures in processing Personal Data in accordance with globally accepted Privacy by Design principles and Fair Information Practice principles.

REVISION HISTORY

Revision Date	Version	Summary of Changes	Approved by
1 December, 2021	1	Initial Version	Publicis Groupe's Chief Data Privacy Officer
19 December, 2022	2	Reviewed, no changes required	Publicis Groupe's Chief Data Privacy Officer
30 October, 2023	3	Reviewed, with revisions for updated US state laws	Chief Data Privacy Officer of Publicis Groupe