DATA HANDLING POLICY

Contents

INTRODUCTION **2**

ACCOUNTABILITY AND IMPLEMENTATION **2**

WHO IS ACCOUNTABLE FOR DATA HANDLING? 2
WHAT IS EXPECTED OF BUSINESS LEADS IN TERMS OF DATA HANDLING? 2
WHAT DATA HANDLING RESOURCES ARE AVAILABLE FOR BUSINESS LEADS? 3

DATA ONBOARDING **3**

WHAT STEPS ARE REQUIRED PRIOR TO ONBOARDING PERSONAL DATA TO PUBLICIS SYSTEMS? 3
ARE THESE STEPS DIFFERENT WHEN ONBOARDING A CLIENT'S PERSONAL DATA? 4

MAINTAINING ACCURACY OF PERSONAL DATA **4**

STEPS TO MAINTAIN ACCURACY OF PERSONAL DATA 4
WHAT SHOULD WE DO IF AN INDIVIDUAL CHALLENGES THE ACCURACY OF THEIR PERSONAL DATA? 5

SENSITIVE PERSONAL DATA **5**

WHAT IS SENSITIVE PERSONAL DATA? 5
DO WE HANDLE SENSITIVE PERSONAL DATA DIFFERENTLY? 5
WHAT ARE THE EXTRA STEPS FOR HANDLING SENSITIVE PERSONAL DATA? 5
WHAT ACTIVITIES ARE PROHIBITED FROM USING SENSITIVE PERSONAL DATA? 6
WHAT ADDITIONAL STEPS ARE REQUIRED FOR HANDLING OF CLIENT PERSONAL DATA THAT IS SENSITIVE PERSONAL DATA? 6

MINORS' PERSONAL DATA **7**

WHAT IS MINOR'S PERSONAL DATA? 7
DO WE HANDLE MINORS' PERSONAL DATA DIFFERENTLY? 7
WHAT ARE THE EXTRA STEPS FOR HANDLING MINORS' PERSONAL DATA? 7
WHAT ACTIVITIES ARE PROHIBITED FROM USING MINORS' PERSONAL DATA? 8
WHAT ADDITIONAL STEPS ARE REQUIRED FOR HANDLING OF CLIENT PERSONAL DATA THAT IS MINORS' PERSONAL DATA? 8

PSEUDONYMIZATION AND DE-IDENTIFICATION **8**

WHAT IS PSEUDONYMOUS DATA AND DE-IDENTIFIED PERSONAL DATA? 8
WHEN SHOULD PUBLICIS PSEUDONYMIZE OR DE-IDENTIFY PERSONAL DATA? 8
STEPS TO PSEUDONYMIZE OR DE-IDENTIFY DATA 9
CAN AND SHOULD PSEUDONYMIZATION OR DE-IDENTIFICATION BE REVERSED, I.E. THE PERSONAL DATA RE-IDENTIFIED? 9

AUTOMATED DECISION MAKING AND PROFILING **10**

WHAT IS AUTOMATED-DECISION MAKING AND PROFILING? 10
MAY PUBLICIS PERFORM AUTOMATED-DECISION MAKING AND PROFILING WITH PERSONAL DATA? 10
GUIDELINES FOR AUTOMATED-DECISION MAKING AND PROFILING 10
ARE ANY AUTOMATED-DECISION MAKING ACTIVITIES PROHIBITED? 11

TRANSFERS OF PERSONAL DATA TO THIRD PARTIES **11**

WHO ARE THIRD PARTIES? 11
WHAT STEPS ARE REQUIRED TO TRANSFER PERSONAL DATA TO A THIRD PARTY? 11
INTERNATIONAL TRANSFERS 12
ARE THERE ADDITIONAL STEPS TO TAKE WHEN THE THIRD PARTY IS A VENDOR? 12
IF A LAW ENFORCEMENT OR REGULATORY AGENCY DEMANDS DISCLOSURE OF PERSONAL DATA, CAN WE PROVIDE THE DATA? 12
ARE THERE EXTRA STEPS TO TAKE IN TRANSFERRING OUR CLIENT'S DATA TO A THIRD PARTY? 13

RETENTION **13**

DATA RETENTION POLICIES MINIMUM STANDARDS 13
STORAGE IN ACCORDANCE WITH DATA RETENTION 13
RETENTION PERIOD 14

EXCEPTIONS TO RETENTION PERIODS 14
DO WE RETAIN CLIENT DATA DIFFERENTLY? 14
DELETION OR DESTRUCTION 14
WHEN SHOULD PUBLICIS DELETE PERSONAL DATA? 14
WHEN SHOULD PUBLICIS DELETE CLIENT DATA? 15
REVISION HISTORY 16
EXHIBIT A: ADDITIONAL RESOURCES FOR DATA HANDLING 17
LAWFUL BASIS FOR PROCESSING 17
PURPOSE LIMITATION 17
EXAMPLES OF PERSONAL DATA CATEGORIES 18
EXAMPLE OF COMPLIANCE DOCUMENTATION FOR UK GDPR 20
LEGITIMATE INTEREST ASSESSMENT 20
TECHNICAL AND ORGANIZATIONAL MEASURES 22
SENSITIVE DATA - APPROPRIATE POLICY DOCUMENT 22
MINOR'S DATA – ZERO DATA DESIGN 23
MINOR'S DATA – FTC COPPA SAFE HARBOR PROGRAM 23
DE-IDENTIFICATION AND PSEUDONYMIZATION 23
AUTOMATED-DECISION MAKING AND PROFILING FLOWCHART 24
VENDOR DILIGENCE QUESTIONS 24

INTRODUCTION

Publicis Groupe and its business units (**"Publicis," "we," "us," "our"**) are committed to handling Personal Data responsibly and in compliance with applicable Data Privacy Law worldwide.

This GDPO *Data Handling Policy (POL-GDPO-152)* (**"Policy"**) (1) supplements and is incorporated into the GDPO *Global Data Privacy Policy (POL-GDPO-151)*, (2) expands the principles set out in Janus and (3) complements the Publicis Groupe's Global Security Office's *Information Classification and Handling Guidelines (GUI-GSO-401)*. This Policy is intended to provide a global baseline across Publicis of practical guidelines for the handling of Personal Data. Should a country, state/province, or local municipality impose legal requirements not covered in this Policy, Publicis will ensure such local requirements are documented in local data handling plans held by Business Units (as defined in the *Global Data Privacy Policy (POL-GDPO-151)*).

Each Business Unit is responsible for documenting and implementing its own local data handling plan consistent with this Policy.

Capitalized terms not otherwise defined herein shall have the meaning assigned in the *Global Data Privacy Policy (POL-GDPO-151)*.

ACCOUNTABILITY AND IMPLEMENTATION

WHO IS ACCOUNTABLE FOR DATA HANDLING?

All Publicis Personnel, however, our Business Leads (see *Global Data Privacy Policy (POL-GDPO-151)*) hold additional responsibilities for implementation and maintenance of Data Handling guidelines.

WHAT IS EXPECTED OF BUSINESS LEADS IN TERMS OF DATA HANDLING?

1. **Understanding** (1) Data Privacy Law, and privacy and security standards in their local market(s); (2) permitted scope of use of Personal Data; and (3) all rights, permissions, or restrictions on the applicable Personal Data.

2. Developing local market **Data Handling Plans** in accordance with this Policy and consultation with GSO, GDPO, and Legal (as necessary).

3. **Sharing** local market Data Handling Plans with Internal Teams **and** conducting **training** as required.

4. In collaboration with local Legal, **aligning contracts** to Policy requirements. Legal shall escalate contractual deviations from this Policy to GDPO and GSO for review and approval.

5. Escalating **deviations** from this Policy to GDPOps, or local GDPO, GSO, or Legal, as appropriate. As needed, local GDPO, GSO, or Legal will escalate to Executive Sponsors.

6. Escalating any matter identified as having a **potential for a legal dispute** related to Data Handling to Legal.

WHAT DATA HANDLING RESOURCES ARE AVAILABLE FOR BUSINESS LEADS?

Technical requirements, best practice guides, and reference links are attached as *Exhibit A*.

DATA ONBOARDING

WHAT STEPS ARE REQUIRED PRIOR TO ONBOARDING PERSONAL DATA TO PUBLICIS SYSTEMS?

1. Confirm **contractual requirements** (*rights, restrictions, processes, timelines*) for Personal Data supplied by a client, Vendor, or other third party.

2. Confirm local market(s)/Business Unit **data handling plan requirements** for onboarding and use of Personal Data.

3. Identify and document **lawful basis or permitted purpose** for the onboarding and use of the Personal Data. If Publicis acts as a Controller of Personal Data, this may include conducting a **Legitimate Interest Assessment**. *See Exhibit A*. Contact your local GDPOps if you have questions about lawful basis or permitted purpose.

4. Document and link the Personal Data fields to Personal Data **categories.** *See Exhibit A*. Consult your local GDPOps for assistance.

5. Identify Personal Data, **document** Personal Data **inventory**, and **map** the **data flows** of the Personal Data and the following:
   a. **Sources** of the Personal Data (could be Publicis, client, Vendor, or other third party);
   b. Intended and actual **disclosures** of the Personal Data from Publicis to a client, Vendor, or other third party;
   c. Intended and actual transfers of the Personal Data from one country to another (generally referred to as an **international transfer** (e.g., Client sends its European CRM data to Publicis in US).
   Please consult with GDPOps for templates.

6. **Limit onboarding and minimize the handling of Personal Data** to only the Personal Data necessary to perform the activities for which the data was collected.

7. Take additional steps related to **Sensitive Personal Data** and **Minor's Personal Data** (*see sections on Sensitive Personal Data and Minor's Personal Data herein*).

8. Document the **data retention timeframe** for such Personal Data (*see Data Retention guidelines herein*);

9. Confirm **technical and organizational measures** in place prior to onboarding in consultation with GSO (*see Exhibit A*).
   a. Use **secure transfer mechanisms** to protect the data in transit (i.e., sending through a secure FTP, encryption in transit, hashing etc.)
   b. **Pseudonymize, anonymize, or de-identify Personal Data, where appropriate.**

10. Document and implement an **Individual request plan** (e.g., Individual access, deletion and opt-out rights). *See Individual Request Policy (POL-GDPO-154).*

ARE THESE STEPS DIFFERENT WHEN ONBOARDING A CLIENT'S PERSONAL DATA?

No; however, if the Client is the Controller of the Personal Data and Publicis is the Processor of the Personal Data, Publicis will only onboard and use the Personal Data in accordance with the instructions of the client, as set out in a written agreement, or otherwise permitted by applicable Data Privacy Law.

Additionally, some Publicis systems are client-facing platforms with self-service Individual request functionality and a custom Individual request plan is not necessary unless Client's instructions conflict with such self-service offering. *Please refer to the Individual Request Policy (POL-GDPO-154).*

MAINTAINING ACCURACY OF PERSONAL DATA

Handling inaccurate Personal Data can be harmful to Individuals and to Publicis and its business units. Personal Data must be kept accurate and up to date by utilizing appropriate processes and protocols that help determine the reliability of the sources we use to obtain Personal Data.

STEPS TO MAINTAIN ACCURACY OF PERSONAL DATA

1. **Ensure the accuracy of any Personal Data we create**. To the extent Publicis compiles Personal Data itself, it must ensure the information is correct. As an example, you give an employee a promotion and pay increase on the basis of an annual increment, the payroll records should be updated to reflect the new salary figure as well as the correct position title and line management in internal directories and systems.

2. **Take reasonable steps to check the accuracy of the data we collect, and we record the source of that data**. A 'reasonable step' will depend on the circumstances and, in particular, the nature of the Personal Data and what you will use it for. The more important it is that the Personal Data is accurate, the greater the effort you should put into ensuring its accuracy. If the Personal Data could have a significant impact on an Individual, independent confirmation that the data is accurate may be necessary. It may be impractical to check the accuracy of Personal Data someone else provides.
   a. Vendors or Clients**.** When obtaining Personal Data from Vendors or clients, we should obtain contractual assurances as it relates to the accuracy of Personal Data.
   b. Publicis platforms. The Business Unit operating a platform that collects or stores Personal Data follow GSO *Information Security Policy (POL-GSO-101)*.

3. **Create a schedule to identify when we need to keep the data updated to properly fulfil our purpose, and update the Personal Data as necessary**.
   a. **Publicis Employees/Contractors**. Encourage Publicis personnel to update their details (e.g., change of address). Routine updates shall be set up by HR. Personal Data should generally be collected directly from the Individual affected.
   b. **Vendors and Clients Contacts**. Personnel of Vendors and clients should be actively encouraged to update their contact details.
   c. **Vendor and Client provided Personal Data**. If the Vendor or client updates its Personal Data on a schedule, implement a scheduled refresh of the data to keep the Personal Data we hold updated as well.

4. **Clearly identify a record of a mistake as a mistake**. If it is necessary to maintain a record of a mistake, ensure that the record is notated as a mistake in order to avoid confusion. As an example, an accounting error resulted in underpayment of wages to an employee. The underpayment should remain documented with a note connecting the underpayment to the correction payment in the payroll records.

5. **Clearly identify a record of an opinion as an opinion**. Where appropriate, record whose opinion it is and any relevant changes to the underlying facts.

6. **In applicable situations and certain geographic regions, offer Individuals the right to correct and carefully consider any challenges to the accuracy of the Personal Data**. See GDPO *Individual Request Policy (POL-GDPO-154).*

WHAT SHOULD WE DO IF AN INDIVIDUAL CHALLENGES THE ACCURACY OF THEIR PERSONAL DATA?

If an Individual challenges the accuracy of his/her Personal Data or asks that the Personal Data be corrected, the Business Unit should consider whether the information is accurate and, if it is not, the Business Unit should delete or correct it. See the GDPO *Individual Request Policy (POL-GDPO-154)*.

SENSITIVE PERSONAL DATA

WHAT IS SENSITIVE PERSONAL DATA?

Personal Data that falls within the "Sensitive Personal Data" category continues to evolve as local markets implement new Data Privacy Law. Sensitive Personal Data is also referred to as *Special Categories of Personal Data* in some local markets. See *Global Data Privacy Policy (POL-GDPO-151)* for the specific definition of Sensitive Personal Data.

Common Personal Data categories that are considered **Sensitive Personal Data** include: racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, health information, sexual orientation, government identification number, account log-in or access credentials, precise geolocation, or contents of private communications (email, SMS, letter).

DO WE HANDLE SENSITIVE PERSONAL DATA DIFFERENTLY?

The handling of Sensitive Personal Data requires heightened data protection measures due to the potential for harm should such data be disclosed. However, the collection and handling of Sensitive Personal Data is a standard business operation of our human resources and financial departments, as such Sensitive Personal Data is needed to fulfil legal and contractual obligations involving our employees.

Where Publicis is not explicitly required to process Sensitive Personal Data, Publicis will limit its use of Sensitive Personal Data, and in some cases, will prohibit the use of Sensitive Personal Data, unless otherwise approved as an exception by Executive Sponsors and GDPO.

WHAT ARE THE EXTRA STEPS FOR HANDLING SENSITIVE PERSONAL DATA?

1. **Identify data fields that qualify as Sensitive Personal Data.** Prior to collection, map the data fields intended to be collected by Publicis.

2. **Ensure legally permitted to process Sensitive Personal Data and individual's consent to process Sensitive Personal Data is obtained in local markets where legally required.** Certain jurisdictions may prohibit the use of Sensitive Personal Data for certain activities or require explicit consent for the collection and use of an Individual's Sensitive Personal Data. Business Lead shall consult local GDPO to determine if

permitted to use Sensitive Personal Data and/or consent is legally required. If required, ensure consent is collected and a record of said consent is retained by the Business Unit. For European Union and UK, please see additional requirements for processing of Sensitive Personal Data in the *Risk Assessment & Mitigation Policy (POL-GDPO-155)*.

3. **Identify Unnecessary Sensitive Personal Data**. Review the Sensitive Personal Data fields to determine what minimum fields are adequate, relevant, and necessary to achieve the specific processing purpose.

4. **Limit onboarding, and data minimization**. Require the source of the Personal Data to remove all unnecessary Sensitive Personal Data from the dataset prior to onboarding to Publicis systems. If the source of the Personal Data is unable to remove all unnecessary Sensitive Personal Data from the dataset prior to onboarding, immediately after onboarding Sensitive Personal Data to Publicis systems, Internal Teams should flag unnecessary Sensitive Personal Data and either delete or hash to render unreadable such unnecessary Sensitive Personal Data.

5. **Pseudonymize, anonymize, or de-identify Sensitive Personal Data,** where appropriate.

6. **Apply risk proportionate Technical and Organization Measures.** See *GSO Information Classification and Handling Guidelines GUI-GSO-401* and Business Unit or Groupe *Technical and Organizational Measures*.

7. **Limit the retention.** Delete Sensitive Personal Data upon the conclusion of its purpose for processing, even if the entirety of the dataset (which may include other non-Sensitive Personal Data) is still in use.

WHAT ACTIVITIES ARE PROHIBITED FROM USING SENSITIVE PERSONAL DATA?

The following prohibited uses may be subject to an exception from GDPO and Executive Sponsors:

1. Inferring or deriving insights from Personal Data where the **inference would be considered Sensitive Personal Data**

2. **Creating inferences** from Sensitive Personal Data

3. **Automated Decision Making** using Sensitive Personal Data

4. **Profiling** using Sensitive Personal Data

WHAT ADDITIONAL STEPS ARE REQUIRED FOR HANDLING OF CLIENT PERSONAL DATA THAT IS SENSITIVE PERSONAL DATA?

1. Business Lead will **engage local GDPO r**egarding any additional legal requirements to be added to a customized Data Handling Plan, if not already addressed in the local/Business Unit Data Handling Plan.

2. Business Lead will **engage local Legal** to review legal risks associated with the services utilizing Sensitive Personal Data.

3. Only handle Sensitive Personal Data that is a **contractual requirement** in the agreement with the Client. *Sensitive Personal Data must be explicitly identified in the written contract and the contract must be approved by Publicis Legal.*

MINORS' PERSONAL DATA

WHAT IS MINOR'S PERSONAL DATA?

Minors' Personal Data is Personal Data of Individuals under the age of 18. Laws in local markets may only restrict the handling of personal data of Individuals under the age of 16 or under the age of 13. Consult GDPO if the following steps in this Minors' Data section can apply only for a segment of minors in a local market.

DO WE HANDLE MINORS' PERSONAL DATA DIFFERENTLY?

Publicis will limit its use of Minors' Personal Data and adhere to extra steps in the handling of such Personal Data.

WHAT ARE THE EXTRA STEPS FOR HANDLING MINORS' PERSONAL DATA?

1. **Identify and map locations or sources where Personal Data will be collected that a minor may visit or otherwise provide Personal Data**, e.g., document all websites, ads, live events, games, and apps that a minor may visit or receive. Flag if the location or source may be of interest or targeted to a minor.

2. **Best practice: do not knowingly collect Minors' Personal Data unless critically require for a business purpose**. Such business purpose may include providing employee benefits to Publicis Personnel. General advertising to minors is not a sufficient business purpose for the collection of Minors' Personal Data. Advertising to minors should be zero-data by design. Internal Teams should actively turn off all data collection and require zero-data settings with Vendors.

3. **Ensure legally permitted to process Minors' Personal Data and explicit consent to process Minors' Personal Data is obtained in local markets where legally required**. Certain jurisdictions may prohibit the use of Minors' Personal Data or require explicit consent from the minor or his/her legal guardian for the collection and use of the Minor's Personal Data. Business Lead shall consult local GDPO to determine if permitted to use Minors' Personal Data and/or consent is legally required. If required, ensure consent is collected and a record of said consent is retained by the Business Unit. *Note: certain state/provincial Data Privacy Law may require parental consent or prohibit certain processing activities, where the federal law only requires Individual consent.*

4. **Identify unnecessary Minors' Personal Data**. If the Minors' Personal Data is not critically necessary to achieve the specific processing purpose, do not collect or onboard the Minors' Personal Data. This may include reducing data fields collected or onboarded.

5. **Limit onboarding and data minimization.** Require the source of the Personal Data to remove all unnecessary Minors' Personal Data from the dataset prior to onboarding to Publicis systems. If the source of the Personal Data is unable to remove all unnecessary Minors' Personal Data from the dataset prior to onboarding, immediately after onboarding Minors' Personal Data to Publicis systems, Internal Teams should flag and delete such unnecessary Minors' Personal Data.

6. I**mplement industry-standard Technical and Organizational Measures**. Certain industry security standards and frameworks for the handling of Minors' Personal Data should be implemented and maintained. Business Lead should consult the GSO for guidance on appropriate measures.

7. **As applicable, utilize Vendors certified by self-regulatory or other seal-of-approval programs related to Minors' Personal Data**. Where such Vendors are not available or applicable, consult with GDPOps Staff to ensure proper diligence is conducted on the Vendor prior to the disclosure to or collection by the Vendor of Minors' Personal Data.

8. **Limit the retention**. Delete Minors' Personal Data upon the conclusion of its purpose for processing, even if the entirety of the dataset (which may include Personal Data of those of age) is still in use.

WHAT ACTIVITIES ARE PROHIBITED FROM USING MINORS' PERSONAL DATA?

1. **Behavioral targeted advertising (profiling) and retargeting.** If legally permitted in the local market, all targeted advertising to minors should be on a contextual basis only and in accordance with applicable data privacy or minors' advertising laws. Consult both local GDPO and Legal for guidance.

2. **Automated-decision making**. See automated-decision making guidelines herein.

WHAT ADDITIONAL STEPS ARE REQUIRED FOR HANDLING OF CLIENT PERSONAL DATA THAT IS MINORS' PERSONAL DATA?

Where our Clients provide Minors' Personal Data or we collect Minors' Personal Data for the benefit of our Clients, Publicis shall:

1. Business Lead will **engage GDPOps** to ensure the intended processing of Minors' Personal Data is sufficiently mapped and documented.

2. Business Lead will **engage local GDPO** regarding applicable Data Privacy Law related to the use of the Minors' Personal Data.

3. Business Lead will **engage local Legal** to review legal risks associated with the services involving Minors' Personal Data. Legal will escalate to **Executive Sponsors for written approval**.

4. Only handle Minors' Personal Data that is a **contractual requirement** in the Client Agreement. *Minor's Personal Data must be explicitly identified in the written contract and the contract must be approved by Publicis Legal.*

PSEUDONYMIZATION AND DE-IDENTIFICATION

WHAT IS PSEUDONYMOUS DATA AND DE-IDENTIFIED PERSONAL DATA?

See definitions in *Global Data Privacy Policy (POL-GDPO-151)*. *Note: De-Identified Personal Data and anonymized Personal Data are referred to as Non-Personal Data in the Global Data Privacy Policy (POL-GDPO-151).*

WHEN SHOULD PUBLICIS PSEUDONYMIZE OR DE-IDENTIFY PERSONAL DATA?

Pseudonymization and de-identification are recognized methods of safeguarding Personal Data, which can reduce the risk to the Individual and may, in certain cases, provide a basis for Publicis to expand the purposes for which Personal Data is used. Publicis endeavors to pseudonymize or de-identify all Personal Data that it does not need or is not obligated to maintain in identifiable form on Publicis systems. Determining when and how to employ these techniques will help Publicis satisfy its obligation for data privacy and security.

In certain local markets, applicable Data Privacy Law may require certain categories of Personal Data to be Pseudonymous or de-identified. Business Leads should consult with local GDPO when developing Data Handling Plans that include pseudonymization and de-identification requirements. For example, health information may be required to be de-identified.

Pseudonymous Data is typically used in connection with targeted advertising, online identity resolution or personalized messaging.

STEPS TO PSEUDONYMIZE OR DE-IDENTIFY DATA

1. **Pseudonymization** is achieved by removing or obscuring direct personal identifiers and any indirect identifiers that could reveal an Individual's identity from each piece of Personal Data in a data set through use of one-way hashing algorithm, which cannot be decrypted. The separated data points should be held in separate databases which may be linked via a key (e.g. a randomized identifier). The "key" will be protected by restricted private cloud access to the key. However, pseudonymization is effectively only a security measure. It does not change the status of the data as Personal Data.

2. **De-Identification** is achieved by removing both direct personal identifiers and indirect identifiers that could reasonably identify, relate to, describe, be capable of being associated with, or be linked to a particular consumer. The Business Unit shall take the following additional steps:

    i. Implement technical safeguards that specifically prohibit re-identification of the Individual to whom the information may pertain;

    ii. Implement business processes that specifically prohibit re-identification of the information, and contractually prohibit downstream recipients from trying to re-identify the information;

    iii. Implement business processes to prevent inadvertent release of De-Identified Data; and

    iv. Make no attempt to re-identify the information, and publicly commit not to try to re-identify the information.

CAN AND SHOULD PSEUDONYMIZATION OR DE-IDENTIFICATION BE REVERSED, I.E. THE PERSONAL DATA RE-IDENTIFIED?

Best Practice: Technical, internal access and authorization controls should be implemented to prevent (i) the re-identification of Pseudonymous Data except as necessary to provide its services, and (ii) any re-identification of De-Identified Data. The following steps should be implemented:

1. **Deidentification**. The steps taken to de-identify data should make re-identification impossible. Therefore, De-identified Data should never be able to be re-identified. If De-identified Data is capable to be re-identified, then it is not truly De-identified Data. Additionally, all third-party contracts should contain representation and warranty from the third party that it will not attempt to re-identify de-identified data.

2. **Pseudonymous data** can only be re-identified in the following circumstances:

    i. Re-identification is required for the services currently being provided to the Client or for Publicis internal business purposes; or

    ii. Re-identification, to the extent feasible, is required in order to satisfy an Individual request.

    All re-identification of pseudonymous data requires the written approval of the CDPO or through the DPIA process. See *Risk Analysis & Mitigation Policy (POL-GDPO-155)* for DPIA process.

    Re-identified Personal Data may only be used within the scope of the initial consent or permissions. Re-identified data generally cannot be used for any secondary purpose unless the data was collected pursuant to a legitimate interest and the purpose is compatible as defined under applicable Data Privacy Law.

AUTOMATED DECISION MAKING AND PROFILING

WHAT IS AUTOMATED-DECISION MAKING AND PROFILING?

Automated Decision-Making is the process of deciding by automated means without human involvement, such as deciding based on digitally created profiles, inferred data, or matching key terms.

Profiling is the automated analysis of an Individual's personal aspects, like behavior, interests, etc., to make a prediction or decision.

MAY PUBLICIS PERFORM AUTOMATED-DECISION MAKING AND PROFILING WITH PERSONAL DATA?

Publicis may provide services that incorporate automated decision-making or profiling for its clients to ultimately provide Individuals with more useful and relevant advertising. Such as programmatic ad buying and interest-based advertising (automated decision-making) and audience segmentation, insights, and consumer profiles (profiling).

However, the use of automated decision-making or profiling can also impact an Individual's rights (a Legal Effect) or significantly influence an Individual's circumstances and choices (a Significant Effect). For example, impairing an Individual's right to vote or automatic refusal of online credit application.

Therefore, such practices are explicitly restricted or otherwise regulated by Data Privacy Law or self-regulatory frameworks in certain jurisdictions globally. Publicis recognizes the risks associated with automated decision-making and profiling and such activities should be performed in accordance with the guidelines herein.

GUIDELINES FOR AUTOMATED-DECISION MAKING AND PROFILING

1. **Determine if Automated-Decision Making will have a Legal or Significant Effect.** If the activity may lead to a Legal or Significant Effect, the Business Unit working with Local GDPO should conduct a data protection impact assessment (DPIA) to determine whether it can provide sufficient safeguards to mitigate the risk to the impacted Individuals. The DPIA addressing the risks should be completed before the Profiling or Automated-Decision Making begins. Please look at the *Risk Analysis and Risk Mitigation Policy (POL-GDPO-155)* for DPIA process.

2. **Be transparent**. Provide a privacy notice publicly available on all applicable websites if Publicis platforms are engaging in profiling or automated decision-making. In some cases where we obtain Personal Data indirectly, a link to the notice should be sent to the Individuals impacted by the automated-decision making. The notice should:

    a. describe the processing activities, including its use of Personal Data for Profiling or Automated Decision-Making;
    b. provide meaningful information about the logic involved in the decision-making process;
    c. explain the consequences of the processing by using plain language and relevant examples;
    d. notify Individuals of their rights under applicable Data Privacy Law, including as applicable, the right to object, obtain human intervention, express their points of view, and to contest decisions. In the event there are limitations in our ability to honor these rights, those limitations will be disclosed as well.

3. **Use de-identified, Pseudonymous, or anonymized data in profiling activities**.

4. **Honor Individual's rights** to object to or withdraw consent, as applicable, for Automated Decision-Making and Profiling, as well as all other Individual rights, as described in the GDPO *Individual Request Policy (POL-GDPO-154)*.

ARE ANY AUTOMATED-DECISION MAKING ACTIVITIES PROHIBITED?

The following prohibited uses may be subject to an exception from GDPO and Executive Sponsors:

Automated Decision Making or Profiling using **Sensitive Personal Data**

The following prohibited uses will never be subject to an exception:

1. Automated Decision Making or Profiling using **Minors' Personal Data**

2. **Credit Eligibility**. Determining adverse terms and conditions of or ineligibility of an Individual for credit.

3. **Health Care Treatment Eligibility**. Determining adverse terms and conditions for or ineligibility of an Individual to receive health care treatment.

4. **Insurance Eligibility and Underwriting and Pricing**. Determining adverse terms and conditions of or ineligibility of an Individual for insurance, including, but not limited to, health insurance.

5. **Preferential Pricing with a Discriminatory Impact**. Offering preferential pricing or offers based on membership in certain protected classes of Individual based on Sensitive Personal Data (e.g. racial or ethnic data, sexual orientation, political affiliation or trade union membership).

TRANSFERS OF PERSONAL DATA TO THIRD PARTIES

Publicis Business Units may transfer Personal Data to third parties on the condition that the third party affords a level of data protection the same or comparable to this Policy, and provided a written contract is in place.

WHO ARE THIRD PARTIES?

Clients, Vendors, business partners, law enforcement or regulatory agencies, courts, and other Individuals and entities. Even other Publicis companies (affiliates of a Business Unit) can be considered a Third Party. Employees receiving and using Personal Data as part of their employment at Publicis, are not third parties.

WHAT STEPS ARE REQUIRED TO TRANSFER PERSONAL DATA TO A THIRD PARTY?

1. Identify Personal Data, **document** Personal Data **inventory**, and **map** the **data flows** of the Personal Data from Publicis to the Third Party.

2. **Transfer is for a permitted purpose**.

   a. If Publicis is transferring the Personal Data for its own purposes (as a Controller), it may only do so in accordance with the purpose it was collected. *See Global Data Privacy Policy (POL-GDPO-151)* for Lawful Basis and Legitimate Purpose.

   b. If Publicis is transferring the Personal Data for another party's purpose (as a Processor), it may only do so in accordance with the contract with the other party. As an example, as part of the services for a client, we need to send a record of our client's customers to a printer so that a direct mail can be sent to those customers.

3. **Limit the data to be transferred**. Ensure we are only transferring the data necessary for the use and purpose. As an example, a printer needs full name and mailing address, so we do not send telephone number.

4. **Identify if the Personal Data will be transferred internationally.** Flag if the data originates in a different country than where it will be transferred, or ask that the source of the data flag the data with country codes. Engage local GDPO to ensure the proper data transfer mechanism (e.g. consent, standard contractual clauses, adequacy) is in place prior to the transfer.

5. **Execute contract between Publicis and the third party**. Prior to transferring the Personal Data, ensure there is a contract in place between the Business Unit and the third party receiving the Personal Data. The contract should include, at minimum, any necessary data transfer mechanisms, identify which Data Privacy Law apply and that the third party will comply with such laws, technical and organizational measures, and if applicable that the third party will only use the data in compliance with Publicis' instructions and limit further use of the data. Please consult local Legal for contract.

6. **Implement encryption in transit and pseudonymize the data**, if possible.

INTERNATIONAL TRANSFERS

International transfers of Personal Data outside Publicis are not allowed without appropriate steps being taken, such as contractual clauses which will protect the Personal Data that is being transferred. It's the responsibility of the Business Unit to ensure that appropriate steps are taken.

Consult local GDPO to determine if there is a restriction on transferring Personal Data from one country to another. This also includes if we are allowing a third party to remotely access the Personal Data.

ARE THERE ADDITIONAL STEPS TO TAKE WHEN THE THIRD PARTY IS A VENDOR?

1. **Vendor Due Diligence**.

   a. **GDPOps**. When the Business Unit is in the contracting phase with the Vendor, it should consult its assigned GDPOps. GDPOps will ask the Business Unit to provide information regarding the Vendor and to require the Vendor to answer certain questionnaires. Vendors that are processing Personal Data are required to complete and submit a data privacy and security questionnaire on an annual basis.

   b. **Business Unit**. Where Vendor due diligence is not centrally managed by GDPOps, Business Leads and Internal Teams should coordinate with local GDPO to develop a process for the applicable Business Unit for Vendor due diligence procedures. Business Leads and Internal Teams should escalate to the Executive Sponsors to obtain sufficient resources.

2. **Vendor Data Processing Agreement**. Publicis Personnel are responsible for identifying Vendors with whom a written agreement detailing instructions for processing of Personal Data, often referred to as a Data Processing Agreement (DPA), may be required under local market law and bringing those Vendors to the attention of Legal who are responsible for negotiating Vendor terms, including DPAs.

   a. **Engage local GDPO for Vendor Data Processing Agreement template**. Certain countries may require or recommend certain contractual provisions; therefore, it is important to use a template specific to the country where the Personal Data will be collected, uses, or disclosed. Legal should consult local market GDPO contacts.

IF A LAW ENFORCEMENT OR REGULATORY AGENCY DEMANDS DISCLOSURE OF PERSONAL DATA, CAN WE PROVIDE THE DATA?

In certain circumstances, we may be required to disclose Personal Data to third parties when required by law, when necessary to protect our legal rights, or in an emergency situation where the health or security of an Individual is endangered. Prior to such disclosures, we must take steps to confirm that the Personal Data is

disclosed only to authorized parties and that the disclosure is in accordance with the *Public Authority Request Policy (POL-GDPO-153)*.

ARE THERE EXTRA STEPS TO TAKE IN TRANSFERRING OUR CLIENT'S DATA TO A THIRD PARTY?

1. **Clients Instructions.** If the Business Unit is a Processor of Client Data, it can only transfer Client Data to a third party in accordance with the agreement between the Business Unit and the client. This means that the Business Unit does not need its own lawful basis to transfer the Personal Data, it is solely following the instructions of the client.

    a. **International Transfers**. Check the agreement between the Business Unit and the client to determine if transfers outside of the EEA are prohibited. If the agreement prohibits such transfers, the client must agree in writing to allow a transfer of Personal Data outside of the EEA.

2. **Data Processing Agreement.** If using the Vendor solely to perform services for our client, check for terms in the client agreement. The agreement between Publicis and the client may provide terms that are required for the Vendor, such as that the Vendor can only collect or use Personal Data for the purpose described in the agreement between client and Publicis. Ensure these terms are in the Vendor agreement. If these terms conflict with the Vendor's collection or use of the Personal Data, contact local Legal or local GDPO. The client may need to contract with the Vendor directly.

RETENTION

Each Business Unit should implement and maintain its own local market Data Retention Policies, in accordance with this Policy, together with or as a standalone policy to its local market Data Handling plan.

DATA RETENTION POLICIES MINIMUM STANDARDS

1. Allocate appropriate **resources** to implement and maintain local data retention plan.

2. Each Publicis Business Unit shall develop and maintain **Data Retention Policies** in accordance with the guidelines set forth in this Policy. Such plan may be on a country, business unit, or product specific level.

3. **Train** personnel on obligations under Data Retention Policies.

4. Implement **technical and organization measures** to implement data retention terms

5. Monitor and **audit compliance** with Data Retention Policies.

6. If a type of document or Personal Data is not listed in your local market Data Retention Policy, please **consult your Legal contact** to determine an appropriate retention period and whether the schedules should be amended to include such documents.

STORAGE IN ACCORDANCE WITH DATA RETENTION

1. The applicable business unit shall **designate the location** of storage retention facilities, and shall assign a responsible person for overseeing delivery of Personal Data to such facilities

2. Personal Data that is no longer required for legal or business reasons, or that has satisfied predetermined data retention periods and that is not subject to a legal hold, should be **disposed** of in a timely fashion in order to reduce costs of storing, indexing and handling unnecessary Personal Data. Publicis Business Leads should ensure that if data is stored in archived systems or as system back-ups (e.g. email back-ups), whether the data can be segregated and disposed of. Business Leads may need to negotiate exceptions to retention period if their IT teams confirm that such data cannot be purged.

3. To the extent Publicis uses Vendors to store or dispose of Personal Data, such **Vendors** must: (a) comply with applicable Data Privacy Law, (b) maintain reasonable and appropriate security controls and safeguards with respect to records in their possession, custody or control; and (c) provide a complete audit trail and certification of the destruction of the Personal Data.

RETENTION PERIOD

Retain Personal Data solely in accordance with the purpose it was collected and any legal requirements to operate business effectively.

There may be legal requirements that require us to retain or dispose of certain Personal Data for specified amounts of time depending on applicable laws in the local market. Such laws may include (but are not limited to) employment laws, tax laws, securities laws, civil rights laws, or Data Privacy Law. Because applicable laws vary by local market, the Business Leads should consult their local Legal and GDPO contacts.

EXCEPTIONS TO RETENTION PERIODS

1. **Legally binding agreements**: Publicis may enter into legally binding agreements that will require Publicis to retain certain types of records for specified periods of time. To the extent that such agreements exist and require retention for periods of time in excess of what is required by applicable Data Retention Policies, the lengthier retention period is controlling.

2. **Exception for lesser standard**: Requests for exceptions to this Policy, including exceptions to any of the retention schedules set forth in any applicable Data Retention Policies, shall be submitted to the CDPO for written approval, and must be supported by facts showing that an exception is warranted.

3. **Legal hold**: As applicable based on local market. *Publicis Personnel should always consult their local Legal and GDPO contacts for guidance, including without limitation in connection with materials for litigation or regarding any request to transfer Personal Data to another jurisdiction for use in a civil litigation or any other proceeding. See the Public Authority Request Policy (POL-GDPO-153).*

DO WE RETAIN CLIENT DATA DIFFERENTLY?

1. **Retention Period.** Publicis should retain Client Data solely for the lesser of (1) the contractual period or other time period identified in the client agreement, or (2) the end of the Services where the Personal Data was used.

2. **Storage**. Client Data shall be stored solely in accordance with this Policy and the client contract. Where there is a conflict between this Policy and the client contract, please notify local Legal.

3. **Vendors**. Where Client data is transferred to Vendors, ensure that the Vendor agreement contains the same retention period and storage requirements as those contained in the client contract. *Best practice*: obtain written confirmation from the Vendor that it has returned or destroyed all Personal Data of Client at the termination of the Vendor's services.

DELETION OR DESTRUCTION

WHEN SHOULD PUBLICIS DELETE PERSONAL DATA?

1. When Personal Data is **no longer needed for the purpose it was collected**, it should be securely destroyed or archived as soon as practical in accordance with GSO policies.

2. The disposal of records that have aged beyond their **business retention requirement** shall be accomplished via an automatic process in accordance with schedules set forth in **Business Unit Data Retention Policies**.

3. In order to avoid any negative inferences that Data is ever destroyed in anticipation of a particular problem or dispute, the destruction of Personal Data shall take place only **in accordance with this Policy** and any applicable Data Retention Policies.

WHEN SHOULD PUBLICIS DELETE CLIENT DATA?

Client data should be returned to the client or destroyed in accordance with the contract between Publicis and the Client. See local Legal for questions about your specific client.

REVISION HISTORY

Revision Date	Version	Summary of Changes	Approved by
1 September 2016	1	Initial Version	Publicis Groupe´s Chief Data Privacy Officer
1 September 2017	2	Reviewed, no changes required	Publicis Groupe´s Chief Data Privacy Officer
1 September 2018	3	Reviewed, no material changes required	Publicis Groupe´s Chief Data Privacy Officer
1 September 2019	4	Reviewed, no material changes required	Publicis Groupe´s Chief Data Privacy Officer
1 September 2020	5	Reviewed and adjusted for the CCPA and the Epsilon acquisition	Publicis Groupe's Chief Data Privacy Officer
1 December 2021	6	Reviewed and revised	Publicis Groupe's Chief Data Privacy Officer
19 December 2022	7	Reviewed, no changes required	Publicis Groupe´s Chief Data Privacy Officer

EXHIBIT A: ADDITIONAL RESOURCES FOR DATA HANDLING

LAWFUL BASIS FOR PROCESSING

You must have a valid lawful basis in order to process Personal Data.

There are six available lawful bases for processing under the GDPR. No single basis is 'better' or more important than the others – which basis is most appropriate to use will depend on your purpose and relationship with the Individual.

You must determine your lawful basis before you begin processing, and you should document it. The UK ICO interactive tool can help you determine the lawful basis.

The lawful bases for processing are set out in Article 6 of the GDPR. At least one of these must apply whenever you process Personal Data:

(a) Consent: the Individual has given clear consent for you to process their Personal Data for a specific purpose.

(b) Contract: the processing is necessary for a contract you have with the Individual, or because they have asked you to take specific steps before entering into a contract.

(c) Legal obligation: the processing is necessary for you to comply with the law (not including contractual obligations).

(d) Vital interests: the processing is necessary to protect someone's life.

(e) Public task: the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.

(f) Legitimate interests: the processing is necessary for your legitimate interests or the legitimate interests of a third party, unless there is a good reason to protect the Individual's Personal Data which overrides those legitimate interests. (This cannot apply if you are a public authority processing data to perform your official tasks.)

PURPOSE LIMITATION

For European Union and United Kingdom:

☐ We have clearly identified our purpose or purposes for processing.

☐ We have documented those purposes.

☐ We include details of our purposes in our privacy information for Individuals.

☐ We regularly review our processing and, where necessary, update our documentation and our privacy information for Individuals.

☐ If we plan to use Personal Data for a new purpose other than a legal obligation or function set out in law, we check that this is compatible with our original purpose or we get specific consent for the new purpose.

For United States:

- Commercial Purpose: to advance a person's commercial or economic interests, such as by inducing another person to buy, rent, lease, join, subscribe to, provide, or exchange products, goods, property, information, or services, or enabling or effecting, directly or indirectly, a commercial transaction.

- Business Purpose (as defined and limited by California Privacy Rights Act): operational purposes provided that the use of personal information shall be reasonably necessary and proportionate to achieve the operational purpose for which the personal information was collected or processed or for another operational purpose that is compatible with the context in which the personal information was collected, and include:

    - Auditing related to counting ad impressions to unique visitors, verifying positions and quality of ad impressions, and auditing compliance with this specification and other standards;
    - Helping to ensure security and integrity to extent the use of consumer's personal information is reasonably necessary and proportionate for these purposes;
    - Debugging to identify and repair errors that impair existing intended functionality.
    - Short-term, transient use, including but not limited to non-personalized advertising shown as part of a consumer's current interaction with the business, provided that the consumer's personal information is not disclosed to another third party and is not used to build a profile about the consumer or otherwise alter the consumer's experience outside the current interaction with the business.
    - Performing services on behalf of the business, including maintaining or servicing accounts, providing customer service, processing or fulfilling orders and transactions, verifying customer information, processing payments, providing financing, providing analytic services, providing storage, or providing similar services on behalf of the business.
    - Providing advertising and marketing services, except for cross-context behavioral advertising, to the consumer, provided that for the purpose of advertising and marketing, a service provider or contractor shall not combine the personal information of opted-out consumers which the service provider or contractor receives from or on behalf of the business with personal information which the service provider or contractor receives from or on behalf of another person or persons, or collects from its own interaction with consumers.
    - Undertaking internal research for technological development and demonstration.
    - Undertaking activities to verify or maintain the quality or safety of a service or device that is owned, manufactured, manufactured for, or controlled by the business, and to improve, upgrade, or enhance the service or device that is owned, manufactured, manufactured for, or controlled by the business.

EXAMPLES OF PERSONAL DATA CATEGORIES

This list is examples of categories of Personal Data used in the United States

Personal Identifiers	Name or Alias, Account Name and number, Address, Email address, Phone number, IP address, Device ID, Ad ID, Online Identifier (Cookie ID), Unique Personal Identifiers, Probabilistic Identifiers, Social media handles, Loyalty number, Social Security number*, Driver's License*, State Identification*, and Passport*
Customer Records	Signature Bank Account # Credit Card #, Debit Card #, or any other financial information

Protected Class	Racial or Ethnic Origin Religious Affiliation or philosophical beliefs Disability (US) Date of Birth, if over 40 years of age (US) Age, if over 40 years of age (US) Gender (US)
Commercial Information	Purchase histories or tendencies Purchase transactions Products or services considered
Biometric Information	Physical characteristics Biological and behavioral characteristics DNA Fingerprint Facial Recognition Voice print Imagery of the iris, retina, vein patterns Exercise/ fitness tracking data Keystroke patterns or rhythms Sleep patterns
Internet and Electronic Network Activity	Internet Activity Abandon Cart/ Abandon Browse Network Information Browser Information Browsing behavior/ Search History Interaction with a website (clicks, views, likes, comments, shares, engagement) Email activity (clicks, opens, conversions) Data collected via Pixels, Cookies, Tags or other tracking technologies (e.g. Website analytics)
Geolocation	Latitude/ Longitude Radius
Audio, Electronic, Visual, Thermal, Olfactory or Similar Information	CCTV Videos Photographs Voice Recordings
Professional or Employment Information	Resume/CV References Disciplinary actions Salary Reviews Background checks/ criminal history
Education Information	Grades Disciplinary Actions Reviews Test Scores IQ Scores
Inferences and Profile Data	Preferences Characteristics Predispositions Tendencies Behaviors Attitudes

	Abilities Inferences made about a consumer Score assigned to consumers

*also considered Sensitive Personal Data

EXAMPLE OF COMPLIANCE DOCUMENTATION FOR EEA AND UK

For Business Unit when collecting and using its own Personal Data: https://ico.org.uk/media/for-organisations/documents/2172937/gdpr-documentation-Controller-template.xlsx

For Business Unit when collecting and using a Client's Personal Data solely in accordance with the client contract: https://ico.org.uk/media/for-organisations/documents/2172936/gdpr-documentation-Processor-template.xlsx

LEGITIMATE INTEREST ASSESSMENT

Legitimate Interest Assessment (LIA)

Some Data Privacy Law, such as the GDPR required Controllers that are relying on legitimate interests to conduct and document a formal legitimate interest assessment – a LIA. Each Business Unit that relies on legitimate interest when processing Personal Data as Controller, is responsible for conducting a LIA to demonstrate and document that the interests or the fundamental rights and freedoms of Individuals are considered and protected, taking into account the reasonable expectations of such Individuals based on their relationship with the Controller. We should maintain a record of the LIA, so we can demonstrate we have considered the rights and freedoms of Individuals. Additionally, Virginia's Consumer Data Protection Act (VCPDA) requires a risk assessment with similar steps as a LIA where a Controller sells personal data, processes Personal Data for targeted advertising or profiling, processes Sensitive Personal Data, or its processing of Personal Data causes heightened risk to an Individual.

Practical Steps for conducting a LIA

The LIA usually consists of a three-part test:

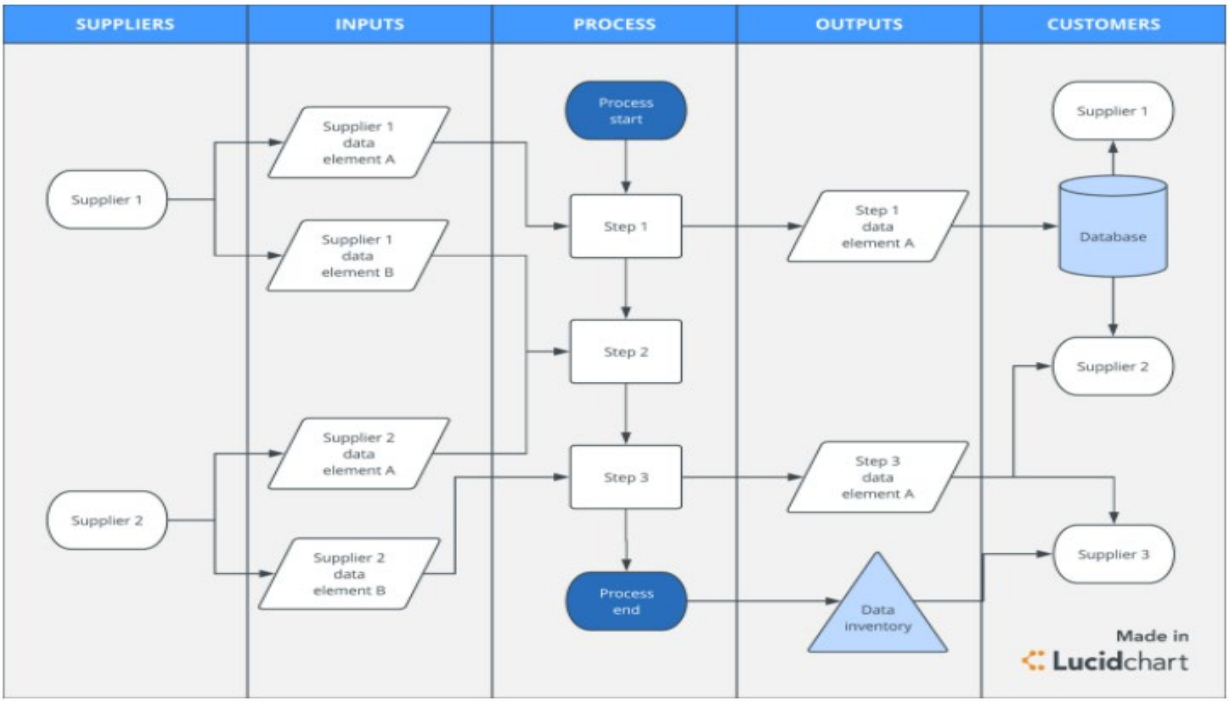
1. **The purpose test** (identify the legitimate interest). In this first step the Publicis Business Unit needs to identify and document the purpose of the processing and decide whether it counts as a legitimate interest. It is important to be as specific as possible, as this helps you when it comes to other parts.
2. **The necessity test** (consider if the processing is necessary). In this second step the Publicis Business Unit must consider carefully whether the processing is actually necessary for the purpose it has identified in step one, and if the purpose can be achieved in any other way, without processing the Personal Data, or less Personal Data.
3. **The balancing test** (consider the Individual's interests). In this last step the Publicis Business Unit needs to consider the interests and fundamental rights and freedoms of the Individual, and whether these overrides the legitimate interests you have identified. There is no exhaustive list of what should be considered when conducting the balancing test, but each Business Unit should as a minimum consider:
    a. the **nature of the Personal Data** it wants to process;
    b. **reasonable expectations** of the Individual; and
    c. the **likely impact** of the processing on the Individual and whether any safeguards can be put in place to mitigate negative impacts

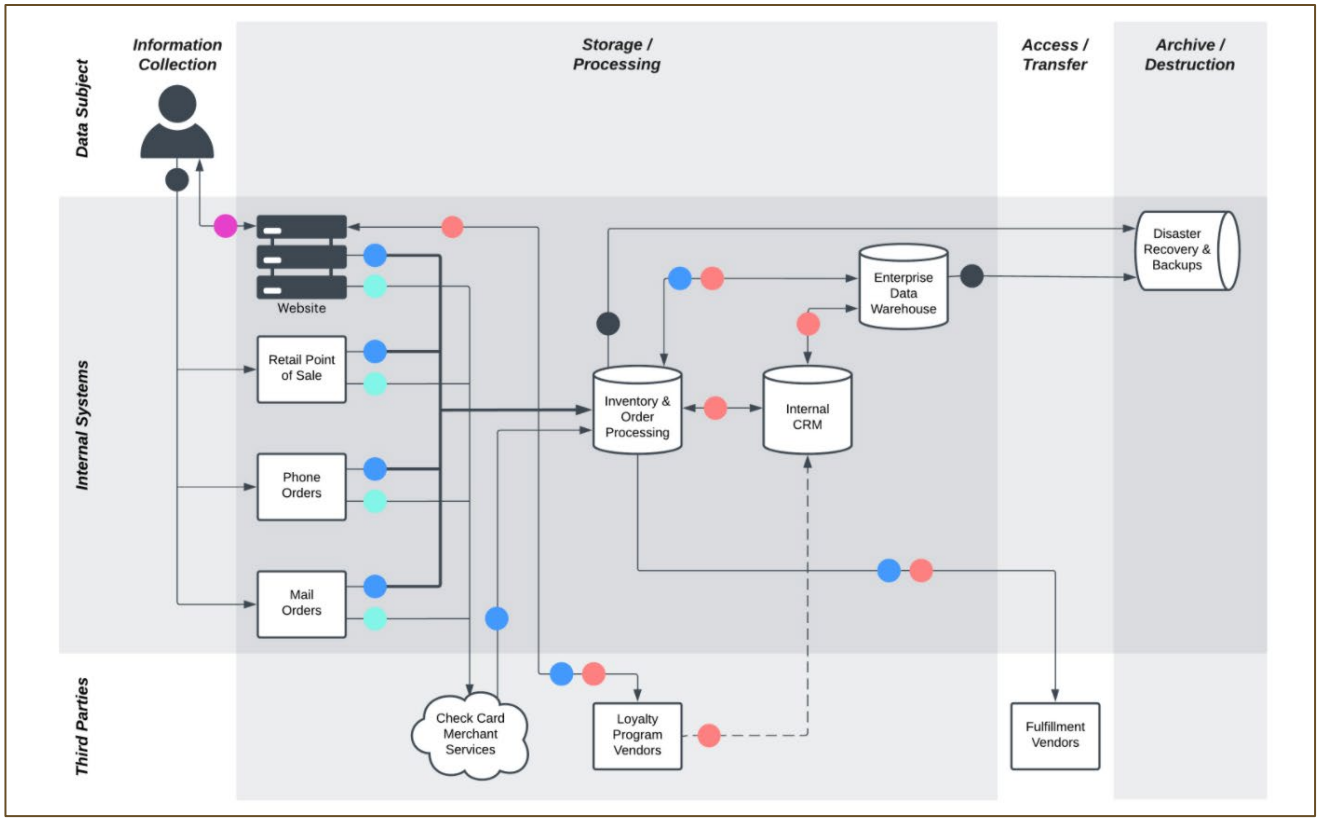
    If the Business Unit intends to process data in ways that the Individual would not reasonably expect, the balancing test may weigh in favor of the Individual, and legitimate interest might not be a lawful basis for the processing.

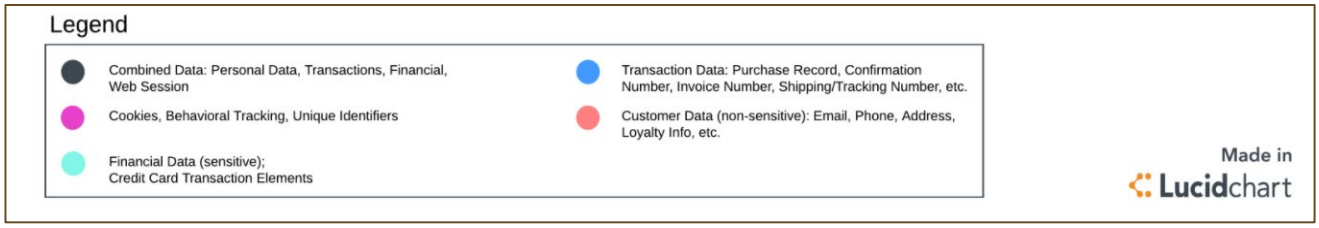
The Publicis Business Unit will consider the following risk mitigation techniques in conducting its balancing test:

- Determining whether to what extent Individuals' rights can be honored.
- Pseudonymizing or de-identifying Personal Data where operationally feasible.
- Hashing Personal Data or providing additional protections such encryption.
- Enforcing a data retention and deletion schedule. Such Data Retention Policy may be on a product level.

Please consult the UK Information Commissioner's Officers guide on legitimate interest assessments for further information, and always contact your local GDPO contact if you believe you need to conduct a LIA.







TECHNICAL AND ORGANIZATIONAL MEASURES

Please contact the GSO for updated versions of the Technical and Organizational Measures for Publicis Groupe.

SENSITIVE DATA - APPROPRIATE POLICY DOCUMENT

https://ico.org.uk/media/for-organisations/documents/2616286/appropriate-policy-document.docx

MINOR'S DATA – ZERO DATA DESIGN

Tags should not include piggyback pixels, ID sync pixels, or other code that could be used to collect Minor's Personal Data. Performance measurement data should not include Minor's Personal Data.

MINOR'S DATA – FTC COPPA SAFE HARBOR PROGRAM

Kidtech Vendors that specialize in child-friendly digital products and technologies certified by self-regulatory or other seal-of-approval programs, including by way of example programs participating in the Federal Trade Commission's COPPA safe harbor program at https://www.ftc.gov/safe-harbor-program.

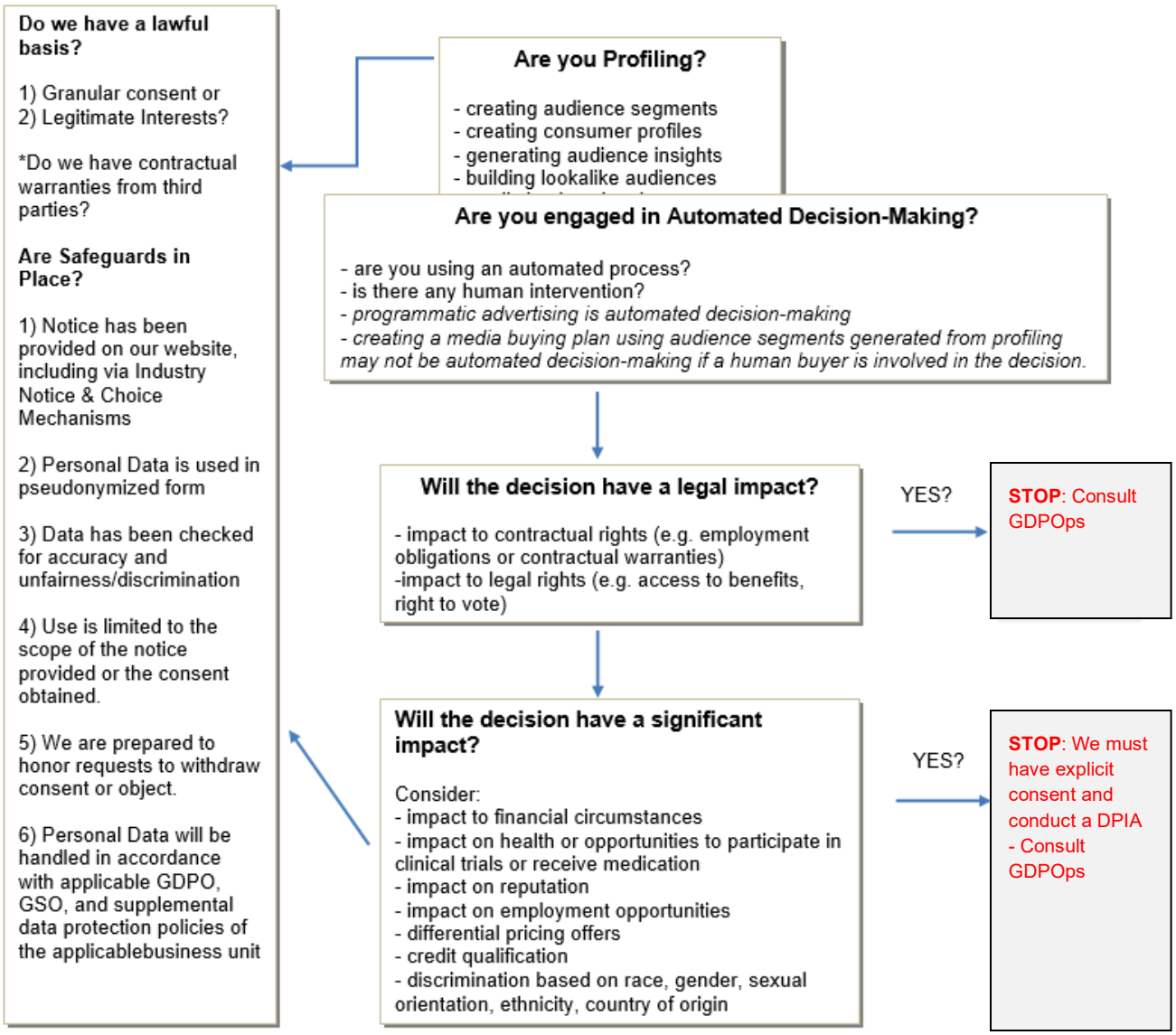
Where Publicis is buying or selling programmatic media, we will utilize all applicable industry standard mechanisms used to screen out Minors' Personal Data, such as the OpenRTB COPPA flag.

DE-IDENTIFICATION AND PSEUDONYMIZATION

Available technical guidance on De-Identification and Pseudonymization includes but is not limited to (i) De-Identification of Personal Information as published by the U.S. Dept. of Commerce National Institute for Standards and Technology (NIST) dated October 2015, and (ii) Article 29 Data Protection Working Party Opinion 05/2014 on Anonymization Techniques dated April 10, 2014.

Should the Personal Data also be subject to HIPPA, utilize the HIPPA deidentification standards. [1] 45 CFR § 164.514(b)(1); 45 CFR § 164.514(b)(2)

AUTOMATED-DECISION MAKING AND PROFILING FLOWCHART



VENDOR DILIGENCE QUESTIONS

We will use commercially reasonable efforts to require Vendors to identify information related to the Vendor's data privacy and security practices as set forth in our data privacy questionnaires, including without limitation:

1. The nature of the Vendor's services;
2. The Vendor's designation under applicable Data Privacy Law;
3. The Vendor's privacy policy;
4. Data privacy/security training for Vendor employees;
5. Insurance coverages;
6. Participation in Industry Notice & Choice Mechanisms;

7. Categories of Personal Data processed;
8. Categories of Sensitive Personal Data processed;
9. Whether the Vendor uses Personal Data for its own purposes;
10. Whether the Vendor is able to facilitate data subject requests;
11. The Vendor's sources of Personal Data;
12. The Vendor's lawful grounds for processing as applicable;
13. The Vendor's use of third party subcontractors
14. Where data is stored and cross-border transfers;
15. How the Vendor shares Personal Data with third parties;
16. Data retention periods;
17. The Vendor's documented data security policies;
18. Technical and organizational measures;
19. Data security certifications;
20. Internal audit procedures;
21. Procedures around malware, penetration testing and vulnerability scans;
22. Access control policies;
23. Encryption policies;
24. Incident response plan; and
25. Backup plan.