P&G Privacy Assessment Guidance

BY TPRM PRIVACY OPERATIONS TEAM

Click on the guide you require

- Privacy assessment (Due Diligence) and general info about P&G's contracts
- About the privacy survey
- Third party privacy classification & Key terms in the Survey
- How to complete & submit the survey
- Criteria to select Data Classification (Controller vs Processor)
- EEA/UK/Brazil data transfer info and requirements
- EEA Data Retention
- Data Categories and when my service DOES NOT include PII/Personal data

Privacy assessment (Due Diligence) and general info about P&G's contracts

Back to main page

What is P&G's privacy assessment (due diligence)?

Our privacy assessment is the process used to identify whether third-party vendors have access to personal data and how it is being handled. This due diligence is performed to understand data flows and put in place the safeguards required to comply with P&G privacy policies, as well as with applicable privacy laws and regulations. This process consists of the following steps:

1. **P&G business owner initiates risk assessment with P&G Third Party Risk Management team.**
2. **Supplier is required to complete the Privacy Survey and will receive support from P&G Third Party Risk Management Team.**
3. **If applicable based on the assessment, contract review and signature between P&G and supplier.**

About the contract completion (if applicable)

1. You will receive the contract in a Word/PDF document to review. If you have any changes, please coordinate with your P&G privacy risk reviewer.
2. Complete the highlighted information (e.g., Legal entity, representative, and details in Schedules).
3. Return to P&G the reviewed or signed copy of the contract for P&G to review and sign it as well.

About the privacy survey

Back to main page

What is the privacy survey?

A privacy survey is a structured assessment designed to evaluate how third-party vendors or partners handle personal data and comply with relevant privacy laws and regulations. This survey typically includes questions about the data types in scope, the nature and scope of the data processing, data collection, storage, processing practices, data transfers, and other questions to help P&G evaluate the vendor or partner's compliance with relevant privacy regulations (e.g., GDPR, CCPA, etc.). Depending on the nature and scope of the services, the vendor or partner may also be asked to complete a separate survey with respect to other risks (Information Security, Antibribery and Anticorruption (ABAC) and Conflict of Interest).

Why is it needed?

A privacy survey is essential in the Third-Party Risk Management (TPRM) process as it helps organizations assess and mitigate risks related to how vendors handle personal data, ensuring compliance with privacy regulations, protecting sensitive information, and safeguarding the organization's reputation. It aids in informed vendor selection and management, allowing us to identify which type of privacy & information security agreements need to be signed while also establishing a baseline for ongoing monitoring and reassessment of third-party relationships considering evolving legal and business landscapes.

Note: This survey should not be confused with the VMD survey nor with other risk related questionnaires. If you have any concerns on other surveys. Feel free to contact the Aravo Chat: Link

Scroll down to see key terms ↓

Third party privacy classification & Key terms in the Survey

Back to main page

Key terms :

- **Business Contact Information:** This typically entails personal information such as name, phone number, email address, etc. that are strictly used to carry out the business relationship between the parties (i.e. the vendor/partner and P&G contacts directly involved in managing the business relationship).
- **Data Controller:** Individual or organization that determines the purposes and means of processing personal data. The data controller is responsible for ensuring that any personal data processed complies with applicable data protection laws.
- **Data Processor:** Individual or entity that processes data on behalf of a data controller. The primary role of a data processor is to handle data as instructed by the data controller, which is the entity that determines the purposes and means of processing personal data.
- **Data Transfer:** Refers to the movement of data from one location to another or accessing data in one location from another. This can involve various contexts, including data being accessed from a different location, transferred between devices, systems, or networks. In the realm of data protection and privacy, the term refers to the transfer of personal data across **borders or between different jurisdictions.** Data transfers may occur when data is transferred by P&G to a vendor, when data is transferred by a vendor to P&G, or when data is transferred by a vendor-to-vendor entities or subcontractors, the specifics of each case which may affect applicable agreements and the parties' respective obligations.

Scroll down to next page

Third party privacy classification & Key terms in the Survey

Back to main page

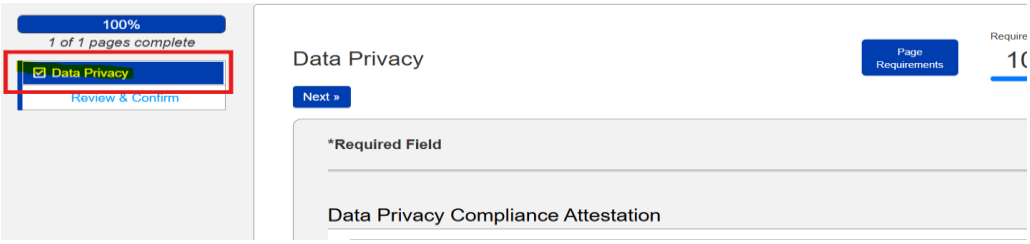
- **Data Sharing:** Refers to the sharing of data between two parties, typically between two independent data controllers.
- **Personal Data (sometimes called PII or personally identifiable data):** Personal data is any information, or a combination of pieces of information, that could be used to identify you or could be associated with a particular individual or household.
- **Processing of data:** Any operation or set of operations performed on personal data, whether automated or manual. This encompasses a wide range of activities that can occur throughout the data lifecycle, including collection, recording, organization, structuring, storage, consultation, restriction, deletion, etc.
- **Pseudonymized data:** Refers to Personal Data that has been processed in such manner that it can no longer be attributed to a specific individual without the use of additional information.
- **Safeguards:** Measures and practices an organization implements to protect personal data from unauthorized access, disclosure, alteration, or destruction. These safeguards are essential for ensuring the privacy and security of personal information and for compliance with data protection regulations.
- **Sensitive/Highly restricted Personal Data:** refers to a specific category of personal data (typically defined under relevant privacy laws) that requires a higher level of protection due to its sensitive nature. This type of data is particularly vulnerable to misuse and can significantly impact an individual's privacy and rights if disclosed or mishandled.
- **SCC's (Standard Contractual Clauses):** Standard Contractual Clauses (SCCs) are legal tools used to facilitate the transfer of personal data from entities within the European Union (EU) to entities outside the EU, particularly to countries that do not have adequate data protection laws as determined by the European Commission.
- **Subcontractor/subprocessor:** Individual or business that is hired by the supplier to perform a specific task or provide a specific service as part of the main project, service or contract.

End of section

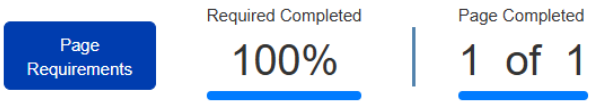
How to complete and submit the survey

Back to main page

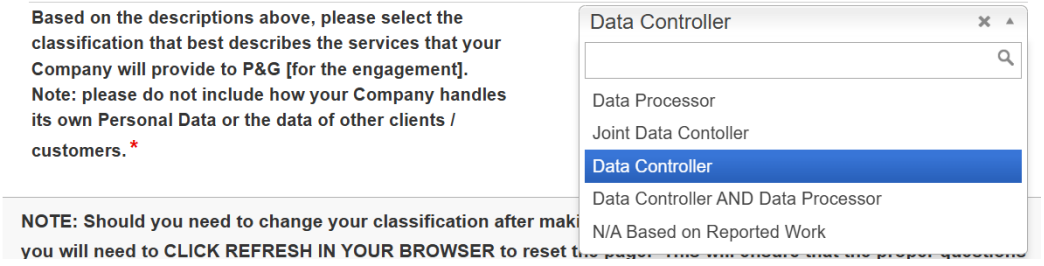
- Step 1: Access the Privacy survey link you have received via email from P&G Aravo <pg@aravo.com>.
- Step 2: Click on the **DATA PRIVACY** page from the MENU BAR to the left:



- Step 3: Scroll down to complete each question on the survey.
- Step 4: To find your progress, at the top-right of the page you will find the percentage. Once it is set to 100% you can proceed to submit:



- Note: Please consider that your responses to the questions below should be given careful consideration, as they may lead to further inquiries or investigation.:



Scroll down to next page

How to complete and submit the survey

Back to main page

- Make sure to add data categories if privacy is on scope as per information shared (more info) and verify if European and/or Brazilian citizens info is to be transferred outside of their jurisdiction (more info):

Select each of the 'Highly Restricted' categories of Personal Data that your Company will collect, acquire, host, use, disclose, access, store, etc. in connection with the services to be provided to P&G. Select all that apply. *

Please select the other types of Personal Data categories that your Company will collect, acquire, host, use, disclose, access, store, etc. Select all that apply. *

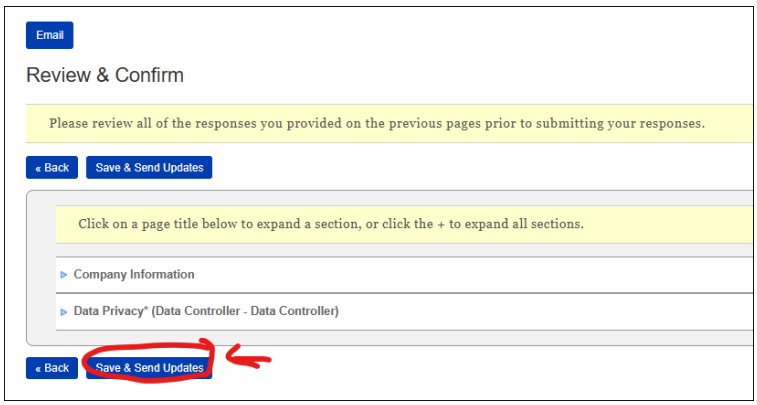
If 'Other' is selected above, please provide a clear description of the category of personal data that your Company manages. *

For the Personal Data in scope for the services provided to P&G, please identify the location(s) of the data subjects from which the Personal Data was originally collected/obtained. Select all that apply. *

- Step 5: After you complete all the questions, Click on **NEXT** button to move to the next page.

« Back Next »

- Step 6: Click on **SAVE & SEND UPDATES** button to submit your answers.



End of section

Criteria to select Data Classification (Processor vs Controller)

Back to main page

Please consider the following before continuing:

1. Ensure to select the correct Data Privacy Classification based on the scope of work that you will provide to P&G.

2. If you are certain no Personal data is to be received, accessed, managed or collected by your company in any way, please select **N/A Based on reported work**. For further reference, visit the following page: Data Categories and when my service DOES NOT include PII/Personal data

3. Please don't select **Joint Data Controller** as this is a special case, before selecting this, be sure to contact the P&G business owner of your services first to align on classification.

4. ***Disclaimer:*** *the below guidance is provided only for general reference purposes and does not account for the specific services you provide to P&G. In the case of doubt, you should consult your company's own privacy or legal team to ensure you select the proper privacy classification under applicable data protection laws.*

5. **Please see a General guide to understand which classification you should select:**

- **Data Processor**

A data processor is a vendor that processes personal data pursuant to P&G instructions. Processing can entail collecting, acquiring, hosting, using, disclosing, accessing or storing. P&G defines the content and scope of any personal data that the Company handles to provide services to P&G. To note, P&G owns this personal data (i.e., data about our employees, our consumers) which is governed by P&G's privacy policy.

- **Data Controller**

A data controller is the organization responsible for making decisions about how Personal Data is used (e.g., where the Personal Data is stored, how it will be used, how long it will be retained, whether the Personal Data will be used for specific purposes, etc.) and is liable for misuse of the Personal Data. A Data Controller determines the purpose for which and the way in which Personal Data is processed and exercises overall control over the "what" as well as the "why" and the "how" of a data processing activity.

EEA/UK/Switzerland/Brazil data transfer info and requirements

Back to main page

❑Regarding personal data obtained from European Union, United Kingdom, Switzerland, Brazil, and Turkey data subjects, please keep in mind the following possible scenarios that are critical to determine the service details:

- If your company manages data from EU/UK/Switzerland but does not transfer this to any jurisdiction outside of the EU/UK/Switzerland. You can select "No" for questions:

Will your Company receive or access Personal Data relating to individuals in the European Economic Area (EEA), UK or Switzerland in, or transfer such data to, any country outside of the EEA, UK or Switzerland (for example receive French Personal Data in the United States)?

- If your company does transfer EU/UK/Swiss data outside of these jurisdictions, please select "Yes" and make sure to select the countries where this data is to be transferred on question:

In what countries/regions will your Company (including transfers through the use of subcontractors) access Personal Data from or transfer Personal Data to? Select all that apply.

- If your company does also manage Brazilian or Turkish data outside of Brazil or Turkey respectively, please make sure of:

1. **Select Brazil and/or Turkey on question:** *For the Personal Data in scope for the services provided to P&G, please identify the location(s) of the data subjects from which the Personal Data was originally collected/obtained. Select all that apply.*

2. **Select countries where the Brazilian and/or Turkish data is to be transferred to on question:** *In what countries/regions will your Company (including transfers through the use of subcontractors) access Personal Data from or transfer Personal Data to? Select all that apply.*

Scroll down to next page for EEA data retention

EEA Data Retention

Back to main page

EEA DATA RETENTION

For European Personal Data data:

- As related to Data Subject Rights noted on the GDPR, consumer data from European citizens retained for more than 30 days needs to be reported to avoid any financial and legal risks related to unauthorized data retention.
- Please connect with either your P&G business contact (if survey has not been received) and align if this is to apply.
- The following question on the survey is strictly linked to the previous:

As part of the service, you are providing to P&G involving Consumer data, do you retain, store or process any personal data for more than 30 days?

Data Categories and when my service DOES NOT include PII/Personal data

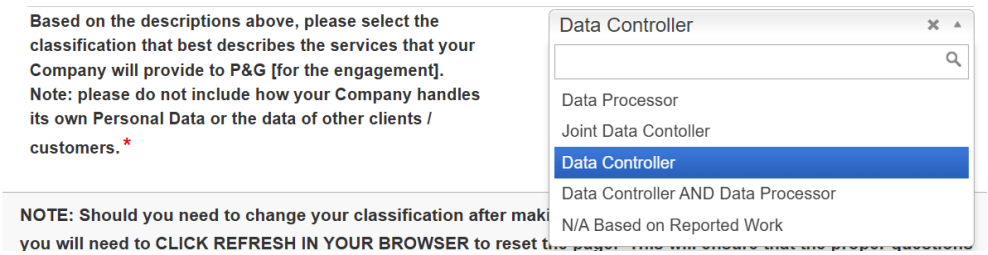
Back to main page

❑In order to consider the service, you provide to P&G as **Out of Scope for the privacy risk**, **YOU MUST AGREE** to the following statements:

- **There's no Personal Data, besides business contact information* , that I collect, use, or otherwise process to provide P&G with my service.**
- **The only personal data I manage is from my employees/subcontractors and I do not transfer this to P&G besides of the business contact information.**
- **No subcontractor manages Personal Data on my behalf for the service I provide to P&G.**

❑If the answer for all is **"Yes"**, follow the instructions noted below:

1. If you received the privacy survey, select **"N/A Based on Reported Work"** on the following question:



2. Reach out to your P&G business contact or to your P&G Third Party Risk Management contact to inform them privacy is out of scope based on the above.

❑ **If the answer is "No"** to the previous statements, please select a classification between Data Processor or Controller (for more info on this click here). And continue with the survey questions.

❑If the privacy survey **was not received**, then confirm with you P&G business contact that no personal data is on scope.

***Business Contact Information:** This typically entails personal information such as name, phone number, email address, etc. that are strictly used to carry out the business relationship between the parties (i.e. the vendor/partner and P&G contacts directly involved in managing the business relationship).*