PRIVACY RISK ASSESSMENT – MARKETING ACTION LIST

UNILEVER GLOBAL DATA PRIVACY

Thank you for completing the Privacy First questionnaire!

You can proceed with your activity upon implementing the required actions below.
It is your responsibility to ensure that the actions below have been completed before your activity starts.

☐ **Privacy Notice**

We must ensure we are transparent with how and why we collect and use personal data. Please make available a link to the Unilever Privacy Policy or a Privacy Notice to inform individuals how Unilever will collect and use their personal data.

☐ **Consent**

We have now fully adopted Enterprise Consent as the standard and ideally all requests should be submitted through campaign wizard. If you are requesting an **exception** or using an **alternative tool,** please review the Marketing Consent Playbook and ensure your Local Data Governance Lead has signed off the look, feel, conditions for consent as well as any legal declarations (failure to do so may result in your data not being usable). If you are based in the U.S., please the U.S. Consent Playbook, and if based in the EU, please follow the Enterprise Consent Playbook.

☐ **Storage and Sharing**

All personal data should be stored within an approved system. Where that's not possible, and you have documents or files containing personal data (e.g., excel or word document), the files must be:

- password protected, and the password should be shared via a separate channel (e.g., if emailing an excel with personal data, you should share the password in a separate email, or via Teams)
- stored on a private SharePoint folder, with restricted access only to individuals on a need-to-know basis.

☐ **Data Retention**

Ensure that we do not retain personal data for longer than needed. You should have a deletion mechanism in place, preferably automated, to delete personal data after an agreed period of time. This should be in line with the Unilever Data Retention Schedules.

☐ **Working with contractors**

If you are working with external contractors, share with them the checklist on how to keep Unilever personal data safe. You can find more information here.

☐ **Transfers**

If your project requires personal data to be shared/transferred or accessed outside of the original market, please work with your local DPA to check that the appropriate legal safeguards are in place.

ADDITIONAL ACTIONS

☐ **Cyber Security Check**

You should engage with the Cyber Security Risk Management Team (previously Information Security) for this project.
You must engage with Cyber Security Risk Management (CSRM) team if you are:

i. using a third party; or
ii. using a new technology or making a substantial change to an existing technology.

For marketing campaigns, this means that you do not need to engage with CSRM if you are only using existing platforms such as Gigya or Epsilon.

Throughout the CSRM engagement process you may be required to engage with various teams that all work together as one to complete your Information Security Assessment and Third-Party Information Security Assessment. The Security by Design consultant will assess who needs to be engaged and will

facilitate these discussions on your behalf, including routing you to the appropriate team if any of the assessments are deemed unnecessary.

We would like to emphasize the importance of initiating the CSRM process as soon as possible, as it functions independently of the privacy procedures. Prompt action will ensure timely completion and alignment with business objectives.

- **Ethics**
  Please refer to the best practice on communicating and setting expectations when using data Communicating and setting expectations on data use and if you have any concerns your concerns that your projects may have data ethics risks then please reach out to our Ethics team enquiries.dataethics@unilever.com.

Should the scope of the activity change, it will be **your obligation to conduct a new Privacy Risk Assessment.**