PRIVACY

GRI 418-1 SASB FB-FR-230A.1, CG-MR-230A.2, CG-EC-230A.2, CG-EC-220A.1, CG-EC-220A.2

We are responsible at all times for protecting and maintaining personal data privacy for our associates, customers, members, and third parties, pursuant to all applicable laws and internal global policies.

Our Privacy Policy sets forth the guidelines so Walmart de México y Centroamérica associates may handle and protect the personal data with which they have access during their daily activities, guaranteeing the privacy, confidentiality, and safety of that information from the moment it is obtained and throughout all stages where it is used.

> This policy also covers the requirements under which the company compiles, uses, processes, and destroys such personal information

For further reinforcement of this, we have a Privacy Notification and a Policy on Maintaining Registries. Each privacy notification describes the data to be gathered and the purpose for said gathering, which is recurrently reviewed to ensure that the purposes for use of personal data are correct and in force.

We have mechanisms available so the owners of personal data may make informed decisions on its use, in addition to the means by which these owners may exercise their rights to access, verify, cancel and object (ARCO).

We have also developed official channels so our associates or third parties may report any leaking of personal data and take immediate action needed to protect said data; and protocols for the rapid and efficient response to cases of data leaks, including an Incident Response Committee, consisting of representatives from key areas in the organization.

Included in the progress made in the field of privacy, in 2021 we implemented a protocol for Privacy Risk Management (PRM) evaluation, which enables us to analyze any data exchange, either internal or with third parties, and to analyze any risks regarding information privacy.

This protocol consists of a questionnaire whose purpose is to analyze, identify, and document privacy risks that may arise with projects involving personal data handling (that is, any information that identifies or makes a person identifiable) with the purpose of mitigating those risks and complying with legal requirements concerning data protection.

This evaluation begins when a detected project, activity, or procedure attempts to use personal data.

Likewise, since guaranteeing the protection of personal data is required, the SSP (Security Solution Plan) process, which is overseen by the Information Security department, is put into action and conducts the necessary reviews to ensure that the technological solutions have the corresponding security protocols, as per the data classification.

As part of the SSP flow, verification is performed to make sure the data processing solution has passed the PRM evaluation, to then be able to grant SSP validation and approval