Norton Privacy Manager – Privacy Notice

This Notice is to be read and applies in conjunction with, and in addition to the Symantec - Norton Global Privacy Statement. It describes the categories of data collected by Norton Privacy Manager ("NPM") and the purposes for which those data categories are processed. It is designed to provide mandatory transparency information both to individual Norton users as data subjects and to Small and Medium Business Norton users as data controllers. Please note that data categories marked with an asterisk (*) are personal data transmitted to Symantec for the purpose of delivering the corresponding product features and service functionalities. All other data categories are collected by the Norton software for processing in a non-identifiable form.

All of Norton's Products and Services are held to the high standards as set forth in the Symantec - Norton Global Privacy Statement. Furthermore, to inform you transparently about the unique characteristics and specific purposes of the NPM product and service, in addition to a description of NPM, this Notice describes the Personal Data we collect and the purposes for which the Personal Data is processed.

If any part or aspect of this Notice is unacceptable to you, then please do not download, install, or otherwise use NPM.

Norton Privacy Manager

Product/Service Description	Data Access and Collection	Data Processing
Norton Privacy Manager protects online privacy and limits your digital footprint by providing private communications, virtual credit cards, anonymized identities, and private browsing within the app.	*1. Information related to phone calls, emails and email addresses, and texting/messages, including communication metadata and cellular location, city, and country code *2. Virtual card transaction information 3. Email certificate information 4. Log information for email address, IP address, and user account 5. App-related usage information	1. Communications information is necessary to provide telephone, email, and app-to-app or SMS/MMS messaging services and measure and track costs of providing the app. 2. User purchase and merchant information is used to process online transactions. 3. Email certificate information is processed for sending encrypted information. 4-5. Log data and usage information is collected to understand app usage and improve the product, such as debugging.