



ORCA Data Privacy Policy Development



ORCA Joint Board
01.14.2019

- 1 Project Background
- 2 Data Policy Framework
- 3 Data User Types
- 4 Next Steps



The ORCA data and information privacy policy covers:

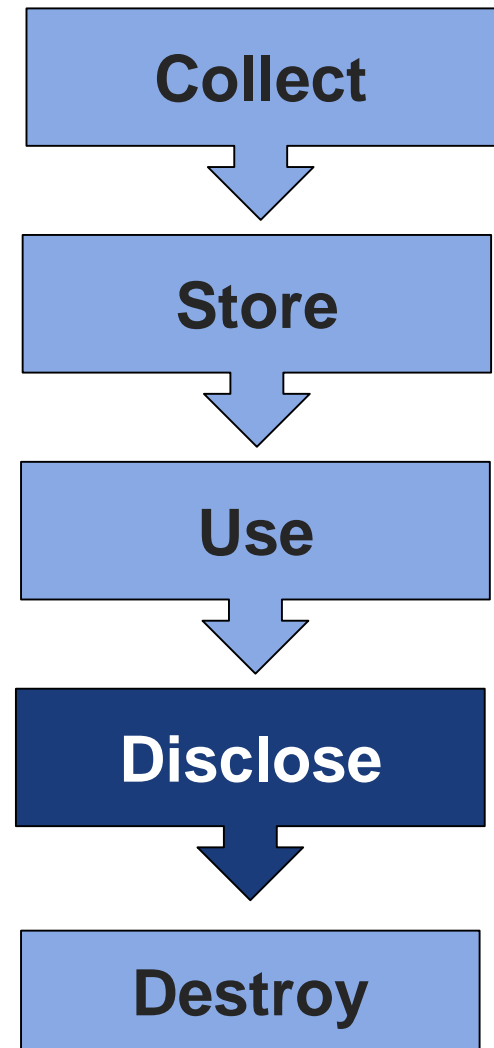
- Data or information provided formally (through an information request) or informally (through an interaction with the ORCA system) pertaining to an ORCA card, including but not limited to:
 - ORCA cardholder information
 - Transaction records
 - Payment information records
 - Customer support records

Information Security:

Protection against unauthorized access, use, disclosure, disruption, modification, inspection, recording or destruction of information.

Information Privacy:

Policies and guidelines related to collecting, using, disclosing, and destroying that personal information.



PECB ISO 29001 White Paper

*"**Personally identifiable information**" means information that can be used to distinguish or trace an individual's identity including, but not limited to, name, social security number, and biometric records, either alone, or when **combined with other personal or identifying information** that is linked or linkable to a specific individual."*

*"**Personal identity information**" means any personal information of a type that is commonly used, alone or in combination with **other information**, to identify or purport to identify an individual."*

- Purpose of data request
- Acceptable data for release
 - Information to be released
 - Appropriate aggregation of data
 - Appropriate anonymization of data
- Permissible uses of the data
- Obligations of requester
- Coverage under current policy



Guiding Principles

- Provide ORCA cardholders with all data tied to their ORCA card.
- Prevent disclosure of ORCA card data to those who cannot establish primary or associated ownership.

Example of User Type 1: Individual customer with a registered ORCA card and associated account

Guiding Principles

- Provide enough data in an appropriate format for business accounts to make meaningful insights.
- Provide data for a time range and aggregation level to prevent misinterpretations or overgeneralizations.
- Ensure that a single ORCA cardholder cannot be identified or tracked through data provided.

Example of User Type 2: Companies that provide their employees with ORCA cards (e.g. Amazon)

Guiding Principles

- Provide data in an appropriate format for internal agencies to make meaningful insights and plan service effectively.
- Ensure that a single ORCA cardholder cannot be identified.
- For reports or datasets that may be made public with original data in a raw format:
 - Ensure that enough data at an appropriate level of aggregation is provided to prevent misinterpretations or overgeneralizations;
 - Ensure that a single ORCA cardholder cannot be identified nor tracked.

Example of User Type 3: Internal agency department that requires ORCA data to plan for service changes

Guiding Principles

- Provide data in an appropriate format to ensure effective research partnerships.
- Ensure that data provided complies with ORCA cardholder consent; without consent, ensure that a single ORCA cardholder cannot be identified.
- Ensure that data provided complies with Institutional Review Board-approved research methods.

Example of User Type 4: Partnerships with universities to measure program effectiveness (e.g. University of Notre Dame for ORCA LIFT)

Guiding Principles

- Provide enough data in an appropriate format for third-party partners to make meaningful insights on program effectiveness.
- Provide appropriate data to support program functionality.
- Ensure that a single ORCA cardholder cannot be tracked.
- Ensure that data provided complies with ORCA cardholder consent; without consent, ensure that a single ORCA cardholder cannot be identified.

Example of User Type 5: MOD Sandbox programs

Guiding Principles

- Provide data for a time range and aggregation level to prevent misinterpretations or overgeneralizations.
- Ensure that a single ORCA cardholder cannot be identified or tracked through data provided.
- Ensure that data provided does not require custom report development or data extraction.

Example of User Type 6: Media requests

Guiding Principles

- Support law enforcement investigations through disclosure of ORCA card data and associated PII when legal requirements for data release are met.
- Ensure that data for more than one ORCA cardholder cannot be provided through a single data request.

Example of User Type 7: Law enforcement organization with warrant on ORCA cardholder

- Draft of ORCA Data Privacy Policy by mid-February.
- ORCA Data Policy scheduled for March 11th Joint Board Action



Questions?

Paul Lavalley – paul.lavalley@ibigroup.com

Jon Campbell – jon.campbell@ibigroup.com

McKenzie Maidl – mckenzie.maidl@ibigroup.com