

**CUSTOMER BIOMETRIC
INFORMATION PRIVACY POLICY
and
CONFIDENTIAL/SENSITIVE
INFORMATION PRIVACY POLICY**

Effective November 1, 2020

McDonough Telephone Cooperative & MTC Communications, Inc. have instituted the following

Biometric Data Defined

As used in this policy, Biometric Data includes “biometric identifiers” and “biometric information” as defined in the Illinois Biometric Information Privacy Act, 740 ILCS14/1 et seq.

“Biometric identifiers” means a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry. It does not include writing samples, written signatures, photographs, human biological samples used for valid scientific testing or screening, demographic data, tattoo descriptions, or physical descriptions such as height, weight, hair color or eye color. Biometric identifiers do not include information captured from a patient in a health care setting or information collected, used, or stored for health care treatment, payment or operations under the federal Health Insurance Portability and Accountability Act of 1996.

“Biometric information” means any information, regardless of how it is captured, converted, stored or shared based on an individual’s biometric identifier used to identify an individual. Biometric information does not include information derived from items or procedures excluded under the definition of biometric identifiers.

Confidential & Sensitive Information Defined

“Confidential and Sensitive Information” means personal information that can be used to uniquely identify an individual or an individual’s account or property. Examples of confidential and sensitive information include, but are not limited to, a genetic marker, genetic testing information, a unique identifier number to locate an account or property, an account number, a PIN number, a pass code, a driver’s license number or a social security number.

Purpose for Collection of Biometric Data

McDonough Telephone Cooperative and MTC Communications, Inc. (hereinafter, “MTC”), collects, stores and uses Biometric Data to test and maintain devices that will be installed on customer premises.

In addition, MTC reserves the right to collect, store and use Biometric Data to allow access to MTC owned property, facilities and equipment.

Video Surveillance

MTC facilities are under video surveillance in public facing locations. The surveillance is in place for protection of MTC property and in public view, so no additional consent will be given or is needed. Video surveillance could be used in a way to collect biometric data; however, MTC is utilizing it only for video surveillance. Surveillance data will be stored in a secure manner, will follow the disclosure requirements in this policy, and will be disposed of in accordance with the record retention schedule within this policy. In accordance with Illinois

law, surveillance does not collect audio.

Policy Implementation

I. Consent

Outside of video surveillance, an individual's Biometric Data will not be collected or otherwise obtained by MTC without prior written consent of the individual. The consent form will inform the customer of the reason the Biometric Information is being collected and the length of time the data will be stored. MTC will not sell, lease, trade or otherwise profit from customers' Biometric Data.

II. Disclosure

MTC will not disclose or disseminate any Biometric Data to anyone without or unless:

- a. First obtaining written customer consent to such disclosure or dissemination;
- b. The disclosed data completes a financial transaction requested or authorized by the customer;
- c. Disclosure is required by state or federal law or municipal ordinance; or
- d. Disclosure is required pursuant to a valid warrant or subpoena issued by a court of competent jurisdiction.

III. Storage

MTC shall use a reasonable standard of care to store, transmit and protect from disclosure any paper or electronic Biometric Data collected. Storage, transmission and protection from disclosure shall be performed in a manner that is the same as or more protective than the manner in which MTC stores, transmits and protects from disclosure other confidential and sensitive information, including personal information that can be used to uniquely identify an individual's account or property, such as genetic markers, genetic testing information, account numbers, PINs, driver's license numbers, and social security numbers.

IV. Retention Schedule

MTC will permanently destroy a customer's Biometric Data when the initial purpose for collecting or obtaining such Biometric Data has been satisfied, OR within three (3) years of the customer's last interaction with MTC, whichever occurs first. Absent a valid warrant or subpoena issued by a court of competent jurisdiction, MTC must comply with its established retention schedule and destruction guidelines.

Contacts

The following office can address questions regarding this Policy:

Holly Fecht, MBA, VP of Business Operations