



## **BIOMETRIC DATA COLLECTION AND RETENTION POLICY - INTERMODAL DRIVERS**

The term “CN” includes Illinois Central Railroad Company, Grand Trunk Western Railroad Company, Chicago Central & Pacific Railroad Company, Wisconsin Central, Ltd., Bessemer and Lake Erie Railroad Company, and Canadian National Railway Company. CN may collect, store, and use Biometric Data for certain purposes described below, and it may disclose that Biometric Data in certain circumstances. This Policy explains what that means for you, and how you consent to CN’s activities.

In signing the Notice and Consent form attached to this Policy, you are providing consent for collection, storage, use, and disclosure of Biometric Data under federal, state, or local laws and regulations that apply to the collection, storage, use, and disclosure of Biometric Data.

CN is providing this Policy in a way that you can retain it for your records. You may download a copy of this policy by visiting <https://www.cn.ca/en/safety/regulations/>, or by scanning the QR code at the kiosk, or by requesting a paper copy from the clerk.

### **What is Biometric Data?**

Biometric Data is based on human features, such as eyes, fingerprints, or voice, that can identify a person. “Biometric Data” as used in this Policy includes both “Biometric Identifiers” and “Biometric Information.”

- “Biometric Identifier” in this Policy means a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry or other physiological traits. Biometric Identifiers do not include writing samples, written signatures, photographs, human biological samples used for 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 healthcare information or information that is protected by the Health Insurance Portability and Accountability Act of 1996 (HIPAA).
- “Biometric Information” in this Policy means any information, regardless of how it is captured, converted, stored, or shared, based on a Biometric Identifier.

### **Collection of Finger Scans and Driver’s License Information.**

CN utilizes an Automated Gate System to increase the efficient movement, and security, of product entering or exiting Illinois terminals. The Automated Gate System utilizes finger scanning technology manufactured by Nascent Technology, LLC and maintained by Remprex Terminal Services, Ltd. along with Remprex, LLC (collectively, “Remprex”).

To utilize the finger scanning technology necessary for a driver to enter or exit Illinois terminals with the Automated Gate System, the driver needs to provide a finger scan, a copy of a driver’s license, and the driver’s commercial driver’s license number before entering the terminal, which will be used by CN for the purpose of authenticating the driver’s entry into and exit from the terminal. The finger scan the driver is providing constitutes Biometric Data.

As part of its maintenance of the Automated Gate System, Remprex will have access to drivers’ finger scan information. It will only access this information to perform the functions required under its services agreement with CN.

### **Storage and Protection of Information**

CN shall use a reasonable standard of care to store, transmit and protect from disclosure any Biometric Data collected. Such 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 CN stores, transmits and protects from disclosure other confidential and sensitive information, including personal information that can be used to uniquely identify an individual such as social security numbers.

Information pertaining to drivers' finger scans will not be disclosed to parties other than CN or Remprex, except in the following circumstances: (1) after CN obtains appropriate written consent from the driver(s); (2) when disclosure completes a financial transaction requested or authorized by the driver(s); (3) when disclosure is required by federal, state, or local law; or (4) when disclosure is required by a valid subpoena or warrant issued by a court. Within CN, the information may be shared with only those employees with a need to know for a specific business purpose.

CN may also disclose information about the driver's entry to or exit from Illinois terminals based on the driver's use of the Automated Gate System, including the fact that the driver provided a finger scan, in response to a request from the motor carrier that a driver works for or contracts with, or under the circumstances listed above or otherwise as required by law.

### **Retention and Destruction of Data**

CN will retain information pertaining to drivers' finger scans during the time that drivers intend to use CN's Automated Gate System. When a motor carrier who is employing or contracting with a driver using CN's Automated Gate System or the driver informs CN that the driver no longer will use the Automated Gate System, CN will within a reasonable period of time permanently delete data pertaining to the finger scan collected from the driver. If a driver or a motor carrier that a driver works for or contracts with does not inform CN that the driver will no longer access CN's Automated Gate System, CN will destroy the data pertaining to the finger scan collected from the driver within 3 years of the date the driver last accessed CN's Automated Gate System.

### **Consent Form**

Before a driver provides his/her finger scan required to utilize the Automated Gate System, the driver must execute the *NOTICE AND CONSENT TO COLLECTION AND USE OF BIOMETRIC INFORMATION* form accompanying this policy.