Alcohol and Tobacco Tax and Trade Bureau

Regulatory MA

Privacy Impact Assessment

Information Collected and Purpose

The Regulatory Major Application System is made up of several component systems, each of which has a specific function for the TTB. These component systems track the status of incoming applications and requests, provide a means to search, retrieve and view approved applications, and stores a variety of information related to product formulations. The component systems within the Regulatory MA only store Personally Identifiable Information (PII) that has been knowingly submitted by individuals to be used for contact purposes.

Information Use and Sharing

The Regulatory MA stores names, email addresses, and phone numbers of individuals who have provided contact information on submitted label certification applications, beverage formula applications, or those individuals who have opened a case with Office of Chief Counsel. Designated and approved TTB employees have direct access to the data stored in the Regulatory MA, but all of those with access receive different rights in according to their job roles and needs.

Information Consent

For an individual's PII to be in Regulatory MA, he or she must have willingly and intentionally filled out and submitted a certificate of label approval application, beverage formula application, or have opened a case with Office of Chief Counsel.

Information Protection

TTB will take appropriate security measures to safeguard PII and other sensitive data stored in Regulatory MA. TTB will apply Department of the Treasury security standards, including but not limited to routine scans and monitoring, back-up activities, and background security checks of all TTB employees and contractors.

In addition, access to Regulatory MA PII will be limited according to job function. TTB will control access privileges according to least privilege, with the most sensitive data, accessible only to one or more system administrator as necessary.

The following access safeguards will also be implemented:

- Passwords expire after a set period
- Accounts are locked after a set period of inactivity
- Minimum length of passwords is eight characters
- Passwords must be a combination of letters and numbers and symbols

- Accounts are locked after a set number of incorrect attempts
- Systems are routinely scanned to ensure that they are configured correctly and have up-to-date patches and virus definitions