Biometric Privacy Compliance Checklist

by David J. Oberly, Squire Patton Boggs LLP

This checklist provides measures for building out a compliance program that generally satisfies U.S. biometric privacy laws and mitigates legal risks associated with the collection and use of biometric data. This checklist includes steps for determining applicability, performing a data inventory, implementing privacy-by-design, drafting a privacy policy, setting data retention/destruction schedules, providing notice, obtaining consent, implementing data security measures, managing vendor/service provider risk, and using arbitration clauses.

For more information on biometric privacy issues, see *Biometric Privacy: Mitigating Legal Risks When Using Biometric Technologies*, *Biometric Privacy State Law Survey*, and *Biometrics Workplace Compliance and Best Practices for Employers*.

Determine Applicability

As an initial step, evaluate whether the company collects or possesses "biometric data" within the scope of applicable biometric privacy laws. You will need to determine:

- Which jurisdictional laws apply to your business
- Whether your business collects data meeting the applicable definition of biometric data

Perform a Data Inventory

If biometric data is collected and/or possessed, complete a data mapping and inventory exercise to determine how and why biometric data is collected, used, and managed. This task involves mapping and inventorying all biometric data that is collected, possessed, used, stored, disclosed, and/or sold, as well as all organizational biometric data processing activities. You will need to:

- Survey all aspects of operations-from marketing to human resources to vendors-to determine all points where biometric data is collected or received from any source
- Map out how that data flows internally after it is collected, including any instances where data is shared with vendors or other third parties, and where data is ultimately stored and maintained within the organization

Implement Privacy-by-Design

Design and implement biometrics programs and services with consumer privacy as a top priority. This principle is commonly known as "privacy-by-design," and involves the embedding of privacy and security measures throughout the biometric technology/data lifecycle such as:

- Establishing default settings that do not require users to take any action to protect their privacy
- Integrating control and transparency into processes to enable consumers to understand the retention, uses, and disclosures of their biometric data
- Offering customers easy-to-use tools to exercise control over their biometric data
- Limiting the collection and use of biometric data to what is necessary
- Collecting biometric data only for specific, explicit, and legitimate purposes
- Not using or processing biometric data in a manner that is incompatible with the purposes disclosed to consumers at the time of collection -and-

- Addressing all biometric privacy-related ethical issues-such as the potential for discrimination and bias-prior to the deployment of biometric technologies

Draft a Privacy Policy

Ensure transparency with customers and other consumers regarding their biometric data practices by implementing a detailed biometrics-specific privacy policy that:

- Gives clear notice that biometric data is being collected, used, stored, and/or shared
- Lists the type(s) of biometric data that are being collected, used, stored, and/or shared
- Explains how biometric data will be used, disclosed, and/or sold
- Describes the security measures used to safeguard biometric data from unauthorized access, disclosure, or acquisition
- Includes the company's biometric data retention and destruction guidelines and schedule
- Strictly prohibits the disclosure of any individual's biometric data without their consent -and-
- Bans the company and its employees from selling or otherwise profiting from any biometric data

Set Data Retention/Destruction Guidelines/Schedules

Privacy policies must include information regarding biometrics-specific data retention and destruction guidelines and schedules.

The specific retention and destruction schedules and limitations vary between today's major biometric privacy statutes. As a best practice, biometric data should be destroyed:

- When the initial purpose for collecting the biometric data has been satisfied
- In the employment context, when the employment relationship has ceased
- At the earliest feasible time

Provide Notice

Provide conspicuous notice regarding the collection and use of biometric data **before** any such data is collected, captured, or otherwise used, including:

- That biometric data is being collected, used, shared/disclosed, and/or stored
- The specific purpose(s) for collecting and using biometric data
- The length of time over which biometric data will be retained or stored
- A brief summary of the protective measures used to safeguard biometric data
- That biometric data may be shared with vendors, service providers, or other third parties (if applicable) -and-
- How individuals can obtain additional information regarding the organization's biometric data practices

Obtain Written Consent

Obtain written consent from all individuals:

- Before collecting any biometric data
- Prior to any subsequent disclosure of biometric data to any third party -and-
- Using a standardized written consent form stating that individuals:
    - Authorize the company to collect, possess, use, store, and share biometric data for the specified purposes

- ○ Have read the company's biometric data policy and notice
- ○ Agree to those policies and the collection/use/sharing of their biometrics

Do Not Sell or Profit from Biometric Data

Adhere to the prohibition on selling or otherwise profiting from biometric data that is a common element among the majority of U.S. biometric privacy laws by:

- • Implementing a no-sale or profiling policy
- • Maintaining mechanisms to ensure no biometric data is sold or otherwise used for profit
- • Educate all employees, agents, and vendors on the company's policy

Implement Data Security Measures

Implement and maintain data security measures to protect all biometric data that is captured, used, possessed, and stored from improper disclosure, access, or acquisition that:

- • Uses reasonable care applicable to an entity's given industry -and-
- • Protects biometric data in a manner that is as or more protective than the manner in which other types of sensitive personal information are safeguarded

Manage Vendor and Service Provider Risk

Take proactive steps to mitigate liability exposure stemming from third-party biometrics vendors, service providers, and related entities by ensuring they maintain the necessary security measures and protocols to safeguard sensitive data while it is in the hands of the vendor or service provider. This includes periodic review and, for those holding sensitive data, third-party audits.

Use Arbitration Agreements and Class Action Waivers

Develop and utilize a robust arbitration agreement and class action waiver to limit potential class action liability exposure with the collection and use of biometric data.

Consult with Experienced Biometric Privacy Counsel

Consult with experienced biometric privacy counsel before implementing any type of biometrics program-or making any substantive modifications to an existing program-to ensure biometric data collection and use practices comply with the current body of evolving biometric privacy laws.

End of Document