

Disclosure to Employees Pursuant to the California Consumer Privacy Act (CCPA)

Notice at Collection for Employees

Effective Date: July 1, 2023

LBS Financial Credit Union (“the Company”) is collecting your personal information and sensitive personal information for human resources, employment, benefits administration, health and safety, and business-related purposes, including for the business purposes listed in the chart below.

We will not sell the personal information we collect. We also will not share it with third parties for cross-context behavioral advertising. We will not sell the sensitive personal information we collect. We also will not share it with third parties for cross-context behavioral advertising. To view our full privacy policy, visit <https://www.lbsfcu.org/california-online-privacy-notice>.

We may collect the personal information and sensitive personal information categories listed in the tables below. The tables also list, for each category, use purposes, and whether we sell the information or share it with third parties for cross-context behavioral advertising. We retain this information for as long as necessary to fulfil the purposes we collected it for, including for the purposes of satisfying any legal, accounting, or reporting requirements. To determine the appropriate retention period for personal information, we consider the amount, nature, and sensitivity of the personal information, the potential risk of harm from unauthorized use or disclosure of your personal information, the purposes for which we process your personal information and whether we can achieve those purposes through other means, and the applicable legal requirements. We may collect, receive, maintain, and use the Personal Information of current and former employees for the following business purposes:

1. To comply with local, state, and federal law and regulations requiring employers to maintain certain records (such as immigration compliance records, travel records, personnel files, wage and hour records, payroll records, accident or safety records, and tax records), as well as local, state, and federal law, regulations, ordinances, guidelines, and orders relating to COVID-19;
2. to evaluate job applicants and candidates for employment or promotions;
3. to obtain and verify background checks on job applicants and employees;
4. to manage the onboarding process;
5. to manage and process payroll and/or Company travel and expenses, employee recognition programs, pay increases and incentives;
6. to administer and maintain group health insurance benefits, 401K and/or retirement plans and to communicate with employees regarding employment-related matters such as upcoming benefits enrollment deadlines, action items, availability of W2s, and other alerts and notifications;

7. to evaluate, make, and communicate decisions regarding an employee’s employment, including decisions to hire, terminate, promote, train, demote, transfer, suspend or discipline;
8. to implement, monitor, and manage electronic security measures on employee devices that are used to access Company networks and systems and the creation, maintenance and security of your online employee accounts;
9. to communicate with employee’s family or other contacts in case of emergency or other necessary circumstance;
10. to manage workers’ compensation claims;
11. to manage employee performance of their job duties and/or employee conduct,
12. to identify potential symptoms linked to COVID-19 (including through temperature checks, antibody testing, or COVID-19 questionnaire), protect employees and customers from exposure to COVID-19, permit contact tracing relating to any potential exposure, communicate with employees and customers regarding potential exposure to COVID-19, and reduce the risk of spreading the disease in or through the workplace;
13. to promote and foster diversity and inclusion in the workplace;
14. to grant and monitor employees access to secure Company facilities, Credit Union Facilities, equipment and systems and maintain information on who accessed the facility;
15. to conduct workplace investigations (such as investigations of workplace accidents or injuries, harassment, or other misconduct) or internal audits;
16. to investigate and enforce compliance with and potential breaches of Credit Union policies and procedures;
17. to engage in corporate transactions requiring review of employee records, such as for evaluating potential mergers and acquisitions of the Company;
18. to maintain commercial insurance policies and coverages, including for workers’ compensation and other liability insurance;
19. to perform workforce analytics, data analytics and benchmarking;
20. to administer and maintain the Credit Union’s operations, including for safety purposes;
21. to exercise or defend the legal rights of the Credit Union and its employees, affiliates, customers, contractors and agents.

Personal Information

Category of Personal Information Collected	Business Purpose for Collection	Sold or Shared	Retention
Identifiers (A real name, alias, postal address, unique personal identifier, online identifier, Internet Protocol address, email address, account name, Social Security number,	All reasons as stated above	No	Up to 7 years from date of termination of employment

driver's license number, passport number, or other similar identifiers.)			
<p>California Customer Records personal information</p> <p>(A name, signature, Social Security number, physical characteristics or description, address, telephone number, passport number, driver's license or state identification card number, insurance policy number, education, employment, employment history, bank account number, credit card number, debit card number, or any other financial information, medical information, or health insurance information.)</p>	All reasons as stated above	No	Up to 7 years from date of termination of employment
<p>Protected classification characteristics under California or federal law</p> <p>(Age (40 years or older), race, color, ancestry, national origin, citizenship, religion or creed, marital status, medical condition, physical or mental disability, sex (including gender, gender identity, gender expression, pregnancy or childbirth and related medical conditions), sexual orientation, veteran or military status, genetic information (including familial genetic information).</p>	1,2,4,6,10,12,13,15,16,18,19, 21	No	Up to 7 years from date of termination of employment
<p>Biometric information</p> <p>(Genetic, physiological, behavioral, and biological characteristics, or activity patterns used to extract a template or other identifier or identifying information, such as, fingerprints, faceprints, and voiceprints, iris or retina scans, keystroke, gait, or other</p>	1,11,14, 15,16,20,21	No	Up to 7 years from date of termination of employment

physical patterns, and sleep, health, or exercise data.)			
Internet or other similar network activity (Browsing history, search history, information on a consumer's interaction with a website, application, or advertisement.)	1,11,14,15,16,20,21	No	Up to 7 years from date of termination of employment
Geolocation data (Physical location or movements.)	1,11,14,15,16,20,21	No	Up to 7 years from date of termination of employment
Sensory data (Audio, electronic, visual, thermal, olfactory, or similar information.)	1,14,15,16,20,21	No	Up to 7 years from date of termination of employment
Professional or employment-related information (Current or past job history or performance evaluations.)	1,2,3,7,11,15,16,19,21	No	Up to 7 years from date of termination of employment
Non-public education information (Education records directly related to a student maintained by an educational institution or party acting on its behalf, such as grades, transcripts, class lists, student schedules, student identification codes, student financial information, or student disciplinary records.)	1,2,3,7,11,15,16,19,21	No	Up to 7 years from date of termination of employment
Inferences drawn from other personal information (Profile reflecting a person's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes.)	1,2,3,7,11,15,16,21	No	Up to 7 years from date of termination of employment

Sensitive Personal Information

Category of Sensitive Personal Information	Business Purpose for Collection	Sold or Shared	Retention
Government identifiers (social security, driver's license, state identification card, or passport number)	All reasons as stated above	No	Up to 7 years from date of termination of employment
Precise geolocation	1,11,14,15,16,20,21	No	Up to 7 years from date of termination of employment
Racial or ethnic origin	1,2,4,6,7,13,15,16,18,19,21	No	Up to 7 years from date of termination of employment
Religious or philosophical beliefs	1,2,7,13,15,16,21	No	Up to 7 years from date of termination of employment
Union membership	1,2,3	No	Up to 7 years from date of termination of employment
Genetic data	1,2,6,13,14,15,16,21	No	Up to 7 years from date of termination of employment
Mail, email, or text messages contents not directed to us	1,2,12,14,15,16,21	No	Up to 7 years from date of termination of employment
Unique identifying biometric information	13,14,15,16,20,21	No	Up to 7 years from date of termination of employment
Health information	1,2,4,6,7,10,12,13,15,16,19,21	No	Up to 7 years from date of termination of employment
Sex life, or sexual orientation information	1,2,7,13,15,16,21	No	Up to 7 years from date of termination of employment

If you have any questions about this Notice or need to access it in an alternative format due to having a disability, please contact us by writing us at LBS Financial Credit Union, P.O. Box 4860. Long Beach, CA 90804-0860, emailing HR@lbsfcu.org or calling 800.527.3328.