BusinessOL.Com, Inc.

CCPA DATA SECURITY POLICY

Definitions

COMPANY	means BusinessOL.Com, Inc.
CCPA	means California Consumer Privacy Act of 2018.
Responsible Person	means Chris Jedlicka
Effective Date	This Policy is effective as of 01/01/2021

1. DATA SECURITY PRINCIPLES

The COMPANY is committed to processing data in accordance with its responsibilities under California law, including with regard to the principles which affirm a right to privacy, provide California residents who are consumers the ability to exercise control over their personal information, provide safeguards against the misuse of their personal information and provide reasonable data security.

Cal. Civ. Code § 1798.81.5, California's data security law, requires businesses that own, license, or maintain personal information about California residents to "implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure." Cal. Civ. Code § 1798.81.5(b).

We are committed to reasonable security procedures and practices, and do so with the following policy provisions.

2. PERSONAL INFORMATION

California's definition of what constitutes "Personal Information" under the data security law is: (1) an individual's first name or first initial and last name in combination with any one or more of the following data elements: (a) Social Security number; (b) driver's license number or California ID card number; (c) account number, credit or debit card number, in combination with any required security access code, or password that would permit access to an individual's account; (d) medical information; (e) health insurance information; and (f) information or data collected through the use or operation of an automated license plate recognition system; or (2) a username or e-mail address, in combination with a password or security question and answer that would permit access to an online account. Cal. Civ. Code § 1798.82(h).

California's definition of what constitutes "Personal Information" under the privacy law (CCPA) is information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household, including but not limited to: (1) identifiers such as a real name, alias, postal address, unique personal identifier, online identifier internet protocol address, email address, account name, social security number, driver's license number, passport number, or other

similar identifiers (2) any categories of personal information described in subdivision e of Section 1798.80 (3) characteristics of protected classifications under California or federal law (4) commercial information, including records of personal property, products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies (5) biometric information (6) Internet or other electronic network activity information, including, but not limited to, browsing history, search history, and information regarding a consumer's interaction with an internet website, application or advertisement (7) geolocation data (8) audio, electronic, visual, thermal, olfactory or similar information (9) professional or employment-related information (10) education information, defined as information that is not publicly available personally identifiable information as defined in the Family Educational Rights and Privacy Act and (11) inferences drawn from any of the information identified in this subdivision to create a profile about a consumer reflecting the consumer's preferences, characteristics, psychological trends, preferences, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes. It does not include publicly available information. For purposes of this paragraph, "publicly available" means information that is lawfully made available from federal, state, or local government records, nor does it mean biometric information collected by a business about a consumer without the consumer's knowledge. Cal. Civ. Code § 1798.140(o)

The COMPANY is committed to provide reasonable security for personal information under each definition.

3. GENERAL PROVISIONS

a. This policy applies to all Personal Information collected, processed, controlled, stored, shared or sold by the COMPANY.

b. "Personal information" has the meaning under both California Code § 1798.81.5(d) and Cal. Civ. Code § 1798.140(o).

c. "Consumer" has the meaning given in the CCPA.

d. "Process" or "Processing" have the meanings given in the CCPA.

e. "Sell," "Selling," "Sale," or "Sold" have the meaning given in the CCPA.

f. The Responsible Person shall take responsibility for the COMPANY's ongoing compliance with this policy.

g. This policy shall be reviewed at least annually.

h. The COMPANY shall comply with an order of the California Attorney General.

4. REASONABLE SECURITY PRACTICES

a. The COMPANY shall implement, document and maintain reasonable security practices and procedures, appropriate to the nature of the information, to protect Personal Information.

b. The COMPANY shall implement all controls at or above the minimum level of information security as defined by the Center for Internet Security's Critical Security Controls applicable to our environment.

5. SECURITY BREACH

a. The COMPANY shall disclose a security breach as expeditiously as possible and without unreasonable delay to a resident of California: (1) whose unencrypted personal information as defined under California Code § 1798.81.5(d) was, or is reasonably believed to have been, acquired by an unauthorized person, (2) whose encrypted personal information under California Code § 1798.81.5(d) was, or is reasonably believed to have been, acquired by an unauthorized person who also acquired an encryption key or security credential that could render that personal information readable or usable or (3) as otherwise required by California or other law.

b. The COMPANY, when required to issue a security breach notification to a California resident, shall meet all of the following requirements: (1) a security breach notification written in plain language titled “Notice of Data Breach;” (2) information under the following headings: “What Happened,” “What Information Was Involved;” “What We Are Doing,” “What You Can Do,” and “For More Information;” (3) a format designed to call attention to the nature and significance of the information it contains; (4) titles and headings in the notice clearly and conspicuously displayed, and (5) the text of the notice no smaller than 10- point type.

c. The COMPANY, in the event of the issuance of a security breach notification to more than 500 California residents as a result of a single breach of the security system, shall electronically submit a single sample copy of that security breach notification, excluding any personally identifiable information, to the Attorney General of California.

d. In the event that a Consumer provides written notice alleging that specific provisions of the CCPA regarding security have been or are being violated and such allegations are found to have merit and curable, the COMPANY shall, within 30 days of such notice, seek to cure the noticed violation, and provide the Consumer an express written statement that the violations have been cured and that no further violations shall occur.