LYNXSPRING®

For the Intelligence of Things™

Disclosure of Personally Identifiable Information Data Breach policy

Lynxspring always endeavors to maintain control of our customer’s personal and operation data stored in our online platforms and applications. We employ measures to protect the confidentiality, integrity, and availability of our customer’s data.

The scope of this policy covers compromises of customer’s personally identifiable information [PII] as described by NIST’s Computer Security Resource Center[1] and related Special Publications[2]. In general, personally identifiable information is “Information that can be used to distinguish or trace an individual’s identity, either alone or when combined with other information that is linked or linkable to a specific individual.”[3] Common examples of PII are full names, email addresses, social security numbers, and usernames. Any non-personally identifiable operational data used in our platforms such as building controls information, energy metrics, history trend data, or similar metrics are not within the definition of PII for this notification policy.

A security breach is defined as an unauthorized third party’s acquisition of any of our customer’s PII maintained and held in Lynxspring’s platforms or applications. Good faith acquisition of personal information by an employee, agent, or business partner is not considered a data breach or compromise.

Lynxspring’s Security Operations Manager, or other designated Lynxspring manger, upon the discovery of a suspected or confirmed breach of our customer’s PII, will notify* our customer’s primary point of contact, or it’s designated IT Support contact, if provided. Notification will be made as soon as practical, but no later than 72 hours** after a PII breach has been confirmed. Notification will be made by email or phone call, or other method if otherwise required by contract.

*Lynxspring staff will make a good faith effort to ensure that any disclosure notification has been received by the intended receiving party, but is not responsible for technical issues such as undeliverable email, unreachable phone reception, or similar communication constraint outside of our control.

**This policy will not supersede any client contracts that may specify a different minimum notification period

[1] https://csrc.nist.gov/glossary/term/PII

[2] NIST SP 800-34 and NIST SP 800-53

[3] NIST SP 800-37 Rev. 2