US Safe Harbor Compliance Statement for Data Privacy

At H.E.L.P. Financial Corporation (HELP), we recognize the importance of securing the private information of our customers, employees, and business partners, and we strive to safeguard the personal information (defined below) we collect and use. This US Safe Harbor Compliance Statement for Data Privacy ("Policy") sets out the privacy principles published by the U.S. Department of Commerce as part of the Safe Harbor Frameworks relating to personal information transferred from the European Union ("EU") and by extension all EEA member countries to the United States.

HELP recognizes the importance of the U.S. - EU Safe Harbor Framework regarding the collection, use, and retention of personal information transferred from the EU to the United States. HELP adheres to the U.S.-EU Safe Harbor Privacy Principles of notice, choice, onward transfer, security, data integrity, access, and enforcement.

HELP complies with these principles in so far as they are applicable to HELP's business. HELP shall not be responsible for the compliance of its customers with the European Commission or the data privacy laws and regulations of any country.

Definitions

Certain words and phrases are defined within this Policy. In addition, the words set out below have the following meaning:

- "EEA" means the 27 EU member states, plus Norway, Iceland and Liechtenstein;
- "personal information" means any information or set of information that identifies an individual, or could be used by or on behalf of HELP to identify an individual. Personal information does not include information which is encrypted or anonymous.

Safe Harbor Privacy Principles

1. Notice – Companies collecting personal data must notify data subjects that they are collecting their personal data, and state the purpose for collecting such data. The company must identify to whom the data will be disclosed and provide notice about how data subjects can contact the company with complaints or questions and how disclosure of their personal information can be limited.
2. Choice – The data subjects must be given a clear and conspicuous choice to opt-out of allowing their information to be disclosed to third parties or used for a purpose which is incompatible with the purpose for which it was originally collected or subsequently authorized by the individual. For sensitive information, data subjects must be given the affirmative or explicit choice whether their information is given to a third party for purpose other than its original purpose or the purpose authorized subsequently by the individual.

3. Onward Transfer of Data to Third Parties – Where a company or organization wishes to transfer information to a third party, it must apply the "notice" and "choice" principles. Where a company or organization wishes to transfer to a third party acting as agent, it may do so if it first either ascertains that the third party subscribes to the Safe Harbor, is subject to the EUD or some other qualifying rule, or enters into a written agreement with the third party requiring the third party to provide at least the same level of privacy protection as is required by the Safe Harbor. If a company meets this requirement, it will not be held responsible if the third party handles data in a way contrary to any restrictions or representations, unless the company knew or should have known that the third party would process the data in such a contrary way and took no reasonable steps to prevent or stop such activity.

   As an alternative, the organization can enter into a written agreement with the third party requiring that the third party provide at least the same level of privacy protection as is required by these principles.
4. Access – Companies must allow data subjects to access their personal data and to correct erroneous information, unless the burden of providing access is greater than the risks associated with the erroneous information or giving access to the information would violate another person's rights. This requirement is subject to the reasonableness standard. In the event a data subject corrects their personal data, Company will ensure such changes are updated in the corresponding records storage at HELP.
5. Security – Companies must take reasonable measures to protect personal information from tampering, destruction, loss, misuse, alteration, disclosure, unauthorized access, and any other potential abuses.
6. Data Integrity – Companies collecting personal data must have reasonable procedures designed to keep the information reliable, accurate, complete, current, and relevant for the lawful purposes for which it was collected.
7. Enforcement – Three elements are required to satisfy this principle: (a) readily affordable and independent recourse mechanisms so that each individual's complaints and disputes can be investigated and resolved and damages awarded where the applicable law or private sector initiatives so provide; (b) procedures for verifying that the commitments companies make to adhere to the safe harbor principles have been implemented; and (c) obligations to remedy problems arising out of failure to comply with the principles. Sanctions must be sufficiently rigorous to ensure compliance by the organization. HELP will cooperate and comply with the EU Data Protection Authorities (DPAs) as the independent recourse mechanism through which HELP will work to investigate any unresolved complaints.