

# DATA PRIVACY & CYBERSECURITY POLICY

## OVERVIEW

At e.l.f. Beauty, Inc. ("e.l.f." or the "Company"), data compliance, processing, protection, and retention are a critical part of our business and risk management processes, and as such, we are committed to compliance with applicable data privacy laws, regulations, internal policies and standards.

We are also committed to transparency and believe in being clear and open with our consumers, particularly regarding the personal data that we collect. Our Privacy Policy is publicly available on each of our brand websites ([e.l.f. Cosmetics Privacy Policy](#), [Well People Privacy Policy](#) and [Keys Soulcare Privacy Policy](#)), and we regularly assess and update these policies to reflect industry practices and applicable laws and regulations.

## PROGRAMS AND PRACTICES

We leverage the National Institute of Standards and Technology (NIST) Cybersecurity Framework as the foundation of our cybersecurity program. We employ benchmarking to understand best practices and industry trends. We conduct security and compliance assessments throughout the year to validate the efficacy of our programs and practices. We also engage an independent third-party expert to assess our cybersecurity posture annually. The results of this yearly assessment are presented to the Board of Directors by our Chief Digital Officer.

To keep pace with ever-evolving threats and industry best practices, we have made and will continue to invest in our information technology systems and personnel.

## TRAINING

We require our employees to complete a security-focused training program to enhance their knowledge of e.l.f. Beauty's data security and protection policies and to enable them to address the threat of cyber-attacks. As part of the program, we require our employees to complete courses on a range of data privacy and cybersecurity topics including security awareness and ransomware, among others.

## OVERSIGHT

This Policy applies worldwide to all employees and partners of e.l.f. Beauty. These principles were approved by the Board of Directors and Executive Team of the Company.

## **MONITORING, AUDITING & VERIFICATION**

Our team adheres to strict compliance requirements to ensure that e.l.f. Beauty is in line with applicable data privacy and protection laws, protecting the rights of staff, consumers and partners. Our Board reviews cybersecurity risks facing e.l.f. Beauty at least annually, including the potential for breaches of our key information technology systems and the potential for breaches of our systems and processes relating to the protection of consumer and employee confidential information.

In the event of suspicious activity, suspected cyberattack, suspected security incident, or possible data breach, all e.l.f. Beauty employees must immediately notify their manager, the IT department and the Legal department to report the incident. We are not aware of any breach or compromise of the personal data of consumers. We have been subject to attacks (e.g. phishing, denial of service) in the past and will continue to evaluate our security practices to best protect our consumers and our data.

*Last updated: September 2022*