



Data Privacy Policy for Employees and Employee Candidates in the European Union

This Data Privacy Policy is effective as of February 1, 2014

1. Data Privacy Policy Overview

- 1.1 Under Armour, Inc. (the “**Company**”) has issued this Data Privacy Policy for Employees and Employee Candidates in the European Union (the “**Policy**”) to explain how the Company handles Personal Information about employees and employee candidates residing in the European Union (“**Employees**”). The Company complies with the U.S. – EU Safe Harbor Framework as set forth by the U.S. Department of Commerce regarding the collection, use, and retention of personal information from European Union member countries (the “**Safe Harbor Framework**”). The Company has certified that it adheres to the Safe Harbor Privacy Principles of notice, choice, onward transfer, security, data integrity, access, and enforcement. Further details about the Safe Harbor Framework and the Company’s certification are available at www.export.gov/safeharbor.
- 1.2 This Policy facilitates the Company’s participation in the Safe Harbor Framework, regulating transfers of Personal Information from the European Union to the United States. The Company will comply with the rules and principles arising under the Safe Harbor Framework.
- 1.3 This Policy governs the Processing of Employee Personal Information relating to Employees ordinarily resident inside the European Union, but whose Personal Information is processed by the Company within the United States.

2. Definitions

In this Policy, the following terms shall have the following meanings:

“**Employee Personal Information**” means any Personal Information that is processed as part of an individual’s working relationship with the Company, for example, pertaining to a current, past or prospective employee of the Company processed in the context of an employment relationship or potential employment relationship with the Company. Such information may include details of any dependents, beneficiaries or other individuals whose Personal Information has been provided to the Company for any purpose, including for any Company benefits plan.

“**Employment Purposes**” means

- **Personnel Management** including but not limited to the normal business practices related to the establishment, maintenance and termination of employment relationships, for example, the Employee’s application for employment, hiring, his or her role and function in the Company, employee management and administration generally (including both during and after employment), employment verification, administering benefits, administering personal short or long term compensation programs, conducting disciplinary proceedings, addressing labor relations issues and processing health insurance claims.

- **Operations Management** including but not limited to establishment, performance and management of business activities of the Company, for example, maintaining and monitoring usage of internal networks and IT systems;
- **Security Management** including but not limited to ensuring the security of the Company's premises and information held by the Company as well as the safety of Company Employees;
- **Legal and Regulatory Compliance** including but not limited to obtaining and releasing Employee Personal Information as required by law (e.g. tax, health and safety, anti-discrimination laws) or judicial authorization and to maintain records that can include Personal Information, such as government identifiers, information relating to sickness, maternity or parental leave, pension and retirement.

"Personal Information" means any information about an identified or identifiable natural person regardless of whether it is held in paper, electronic or any other format, including:

- **Identification Data**, e.g. name, personal address, personal telephone number, personal e-mail address, date of birth, national insurance number, photograph, marital/dependent status and emergency contact information;
- **Information Concerning Employment**, e.g. salary, work and compensation history, planned salary, earnings, career development, paid time off, salary grade, performance information (including performance appraisal, internal communications regarding performance and attendance records), decisions to offer employment, CVs, résumés, applications, employment references and background verification information;
- **Financial Information**, e.g. bank account numbers, tax-related information, and salary-related information;
- **Sensitive Personal Information**, e.g. information which may reveal race or ethnic origin (e.g. for employment equality purposes), religious or philosophical beliefs, or trade union membership, or that concerns health; and
- **Other information** necessary for the Company's business purposes which may be voluntarily disclosed by individuals to the Company during an employment with the Company.

"Process or Processing" means any operation or set of operations that are performed upon Personal Information, whether done by automatic means or otherwise. It includes collecting, recording, storing, organizing, adapting, altering, retrieving, consulting, using, disclosing or making available, destroying and/or deleting Personal Information.

3. General Policy

3.1 Notice to Employees Residing in the European Union

3.1.1 The Company will provide this Policy to Employees through appropriate communication channels to inform them about the purposes for which it collects and

uses their Employee Personal Information, the types of third parties with which it shares their Personal Information, the choice and means the Company offers employees for limiting the use and disclosure of their Employee Personal Information, and how to contact the Company where they have issues or concerns about their Employee Personal Information.

- 3.1.2 The Company may hold and may in the future collect Personal Information about Employees for Employment Purposes.

3.2 Procedure of collecting Employee Personal Information

Employee Personal Information may be collected or accessed in a number of ways, including:

- 3.2.1 directly from the Employee (whether in writing or verbally);
- 3.2.2 generated by the Company in conversations, correspondence, appraisals, etc.;
- 3.2.3 received by third parties so that such third parties may administer the employment application process, benefits, payroll or provide other services for Employment Purposes on behalf of the Company;
- 3.2.4 through the use of Company office, computer and telephony equipment, including mobile phone, smart phones and tablet devices, and software, including electronic messaging, e-mail and internet applications.

3.3 Processing for Employment Purposes

- 3.3.1 The Company will not Process Employee Personal Information for purposes other than the Employment Purposes as set out in this Policy without first informing Employees and giving them the opportunity to object to such Processing. The Company will not Process Employee Personal Information that qualifies as Sensitive Personal Information for purposes incompatible with those given in this Policy unless the Employee in question has explicitly consented to the Processing or the Processing is:

- (a) necessary for administering justice or for exercising statutory, governmental, or other public functions;
- (b) necessary for the establishment of legal claims or defenses;
- (c) in the vital interests of the Employee or another person;
- (d) required to provide medical care or diagnosis; or
- (e) necessary to carry out the Company's legal obligations in the field of employment law.

- 3.3.2 The Company will Process only Employee Personal Information that is relevant taking into account the Employment Purposes for which it is to be processed. Where

Processing of Personal Information is not for Employment Purposes, the Company will obtain the individual's consent prior to the Processing. The Company will not Process the Personal Information more than necessary in the circumstances.

3.4 **Accuracy, retention and protection of Employment Information**

3.4.1 The Company will employ reasonable means to keep Employee Personal Information accurate, complete, up-to-date and reliable for its intended use.

3.4.2 With limited exceptions, Employees will be permitted to review and, where inaccurate, correct Employee Personal Information. The Company will amend the Employee Personal Information or, where the Company considers that the Employee Personal Information is accurate, the Company will include in the file the alternative text that the Employee believes to be appropriate alongside the original information. If it is determined that Employee Personal Information needs to be updated or corrected, the Company shall use reasonable efforts to inform relevant third parties which were provided with inaccurate information.

3.4.3 The Company may not give Employees the ability to review Employee Personal Information where the burden or expense of doing so is disproportionate to the risks to their privacy in a particular case. Where the Company does not provide Employees with the ability to review their Employee Personal Information, it will give specific reasons for refusing to do so and provide a contact point for further inquiries. The Company will, in any event, comply with all applicable local regulations and ensure that Employees can review any Personal Information they have a right to access under the law applicable in their country of residence.

3.5 **Transfers to Group Companies and Company Affiliates**

The Company may disclose Employee Personal Information to group companies and Company affiliates where such entities need to Process that Personal Information for business or business efficiency purposes ("**Intra Group Transfer**"). The Company will ensure that it will protect any Personal Information disclosed during an Intra Group Transfer in accordance with the provisions of this Policy.

3.6 **Transfers to Agents and Contractors**

The Company may disclose Employee Personal Information to third party agents or contractors that supply services to the Company which require the Processing of that Employee Personal Information. The Company will only transfer Employee Personal Information where the agent or contractor has provided written assurances to the Company that it will protect any Employee Personal Information disclosed to it in accordance with the provisions of this Policy. If the Company has knowledge that an agent or contractor is Processing Employee Personal Information in a manner contrary to this Policy, it will take all reasonable steps to prevent or stop the Processing.

3.7 **Transfers to Independent Third Parties other than Agents and Contractors**

- 3.7.1 The Company will disclose Employee Personal Information to third parties other than those mentioned in Section 3.6 above only if required by law or legal process (including disclosures to law enforcement authorities in connection with their duties), to protect the interests of the Company and/or its employees, if there is an emergency situation involving the health and safety of an Employee, or where necessary for the Company to perform a contractual obligation owed to an Employee or for other lawful purposes.
- 3.7.2 Except where the disclosure is required by local law, regulation or court order or where the transfer is necessary to perform contractual obligations owed to the Employee, an Employee will be entitled to object to having their Employee Personal Information disclosed to independent third parties. Except in cases set out in Section 3.3.1 of this Policy, if the Employee Personal Information qualifies as Sensitive Personal Information, the Company will seek consent from Employees before making such disclosures.

3.8 Protection of Employee Personal Information

- 3.8.1 The Company will use appropriate administrative, technical, personal and physical measures to safeguard Employee Personal Information against loss, misuse, unauthorized access, theft, modification, disclosure and destruction. The Company will restrict access to Employee Personal Information under its control to those employees, agents and contractors of the Company who have a legitimate business need for such access.
- 3.8.2 The Company will provide training to Employees and third parties where relevant to promote awareness of the Company's requirements and policies surrounding protection and security of Employee Personal Information.

3.9 Resolving data privacy concerns

- 3.9.1 The Company will maintain a program to ensure compliance with this Policy. The Company's Human Resources Department is responsible for implementing and overseeing the administration of this Policy. All Company employees whose responsibilities include the Processing of Employee Personal Information are required to adhere to this Policy and any implementing policies. Failure to do so is deemed a serious offence, for which disciplinary action may be taken, potentially resulting in termination of employment. Equally, the misuse of Employee Personal Information by an individual or organization acting as agent or service provider to the Company is deemed a serious issue for which action may be taken, potentially resulting in the termination of any agreement.
- 3.9.2 The Company will assist Employees in protecting their privacy and will provide Employees with opportunities to raise concerns about the Processing of their Employee Personal Information. Employees who have concerns about the Processing of their Employee Personal Information should notify their local Human Resources Department. Any submitted complaints will be resolved in accordance with the Company's formal complaints procedures.

3.9.3 If efforts to resolve a concern within the Company are unsatisfactory, Employees may contact the panel of EU data protection authorities established as an independent recourse mechanism under the U.S. – EU Safe Harbor Framework. The Company will cooperate in the resolution of any such inquiries and will comply with any decision or advice issued by the relevant data protection authorities.