Table of Contents

1. Objective

This policy introduces adidas' ambition for privacy, defines the privacy principles to which we will adhere and introduces the Privacy Framework for adidas.

Failure to proactively identify, assess, manage and mitigate related risks might lead to breach of rights or expectations of our consumers, employees and partners. This could result in breach of applicable law or legislation, negative brand perception, reputational damages, significant administrative fines or even in a loss in share price.

2. Scope

The policy is applicable to the entire corporation regardless of brand, legal entity, market, channel or function. Moreover, it sets out expectations on how our third-party suppliers must manage Personal Information for and on behalf of adidas.

Any breach may be treated as a serious disciplinary or contractual misconduct and may therefore be subject to further actions in accordance with applicable mandatory or statutory provisions.

3. Policy

3.1 Privacy Commitment

adidas is committed to comply with all relevant privacy laws and regulations. We will identify and close privacy gaps to meet this commitment.

3.2 Privacy Principles

The Privacy Framework will govern our use of Personal Information to meet the above privacy commitment. The following internationally recognized best practice privacy principles are an entire part of our Privacy Framework and shall be applied in the light of applicable local privacy law and regulation:

Accountability: The Global Privacy Framework will ensure alignment between business strategy and these privacy principles and keep record of how we implement the Executive Board's Privacy Commitment.

Lawfulness & fairness: We are committed to lawful and fair processing that is open and transparent and ensures that individual rights can be effectively exercised.

Purpose specification & limitation: We will ensure collection and use is limited to appropriate and defined purposes.

Data minimisation: Personal Information we collect will be limited to meet the purpose of the collection and we will consider pseudonymization if/wherever appropriate.

Use & disclosure: We will establish a culture and practice of respecting privacy in the way we use and share Personal Information within adidas and with third parties.

Security: We will implement appropriate technical and organizational safeguards to assure integrity, availability and confidentiality of Personal Information we store and process.

Data management: Our data management capabilities will ensure adequate data quality, avoid excessive data retention and enable privacy principles from a technical perspective.

3.3 Organizational and procedural privacy requirements

The following procedural requirements shall be implemented to incorporate the privacy principles above:

3.3.1 Privacy Risk Management

Privacy risks will be identified in accordance with the Global Risk Management System. Privacy risks shall be managed by the appropriate Privacy Action Owner with support from the Privacy Coordinator as appropriate.

3.3.2 Privacy Impact Assessment

Any activity which could or does involve the processing of Personal Information must complete a Privacy Impact Assessment to:

- identify significant privacy risks in High Risk Processing Activities;
- define measures to mitigate these risks;
- identify further privacy requirements imposed by local law or regulation; and
- convert risk mitigating measures and further requirements or opportunities into comprehensive implementation criteria to be signed-off and implemented by the Privacy Action Owner.

3.3.3 Data Processing Register

The Global Privacy Officer shall create and implement a framework to document the processing and lifecycle of Personal Information under privacy and data protection criteria (Data Processing Register) and Privacy Action Owner shall ensure an up-to-date documentation of every Personal Information processing activity within his or her scope.

3.3.4 Privacy in supplier management

We will only engage third party suppliers to process Personal Information for and on behalf of adidas, if

- they are selected based upon their capability to meet adidas' privacy and security expectations;
- they sign onto processing agreements as appropriate (e.g. Data Processing Agreements); and
- their activities are monitored during their engagement to ensure compliance.

3.3.5 Approach to the rights of the individuals

Appropriate procedures must be in place to support individuals to exercise their rights regarding their privacy (such as subject access requests, rectification of their Personal Information or un-subscription, etc.).

3.3.6 Privacy Breach Management Process

Global Privacy Officer shall establish a process or refine existing processes to ensure that in the event of a Privacy Breach the following steps can be taken:

- effective identification of the Privacy Breach;
- a privacy risk assessment completed by Global Privacy;
- mitigation actions will be identified and implemented by relevant stakeholders; and
- relevant stakeholders notified as appropriate, i.e. but not limited to Data Protection Authorities or affected individuals.

3.3.7 Training and Awareness

Global Privacy Officer shall enable and empower our employees to deliver the privacy commitment, e.g. through awareness activities, trainings or privacy related events.

3.3.8 Privacy Coordinators

Privacy roles shall be assigned as required per applicable law (Data Protection Officer or similar) or as further deemed appropriate also acting as Privacy Coordinators within their functional, regional or legal entity scope.

3.4 External stakeholder management

The Global Privacy Officer shall support Government Affairs as appropriate to enhance the external stakeholder management strategy by:

- defining key privacy policy positions to support our business needs key privacy related regulatory activities;
- participating in key industry associations and other platforms influencing privacy policy; and
- adequately cooperating with Data Protection Authorities when they request information, make enquiries and or have privacy related implementation recommendations.

3.5 Assurance and compliance measurement

The Global Privacy Officer shall, to the extent possible and appropriate, align the Privacy Framework with existing assurance frameworks (such as Global Internal Controls and Corporate Internal Audit) and develop additional privacy compliance reporting schemes where necessary.

3.6 Reporting

Global Privacy Officer shall provide regular reports to the Executive Board, at least every 4 months, on privacy related topics including:

- the maturity of the implementation of this policy,
- update on the global privacy risk landscape (risks, mitigation activities, etc.)
- relevant operational KPIs of the Privacy Management System, such as (i) number of Privacy Breaches, (ii) number of Privacy Impact Assessments, (iii) number/percentage of employees being trained on privacy and (iv) number, type and impact of enforcement activities (audits, instructions, fines, etc.)

Privacy Coordinator shall, at least on a quarterly basis, provide the Global Privacy Officer reports as per the reporting framework provided by the Global Privacy Officer and shall, to the extent required under applicable law, further report to the appropriate level of local or functional management.

3.7 Roles & responsibilities with the Global Privacy Framework

Please refer to Appendix 1.

4. Further Information

4.1 Change History

Describe the changes to previous versions / modifications in table form

*Document number**	*Document date*	*Effective date*	*Changes*
1.0	13.10.2018	1.11.2018	Initial Version; Approval by Paul Ehrlich, General Counsel

*consists of [version.modification]:

Version: substantive new content
e.g. additional rule, fundamentally changed subject

Modification: enhancements in content, editorial corrections and reviews without significant change
e.g. typos, wording, improved explanation

4.2 Terms & Abbreviations

For a glossary please refer to Appendix 2.

5. Referenced policies

The following policies should be read in conjunction with this policy:

- adidas Fair Play Code of Conduct
- CM-01 Compliance Policy
- GRM01 Global Risk Management
- GIT-23 Information Security Management System
- GIT-36 Incident Response
- GP-01 Global Procurement Policy

6. Exception handling

Any deviation from this policy requires prior approval of the Privacy Policy Owner.

7. Policy contact

For any questions or further information please contact:

Dr. Falk Boehm
Global Privacy Officer
falk.boehm@adidas.com

Appendix 1: Roles & responsibilities

Executive Board: The Executive Board of adidas AG is ultimately accountable for adidas to comply with applicable privacy laws and regulation.

Privacy Policy Owner: The person, who the Executive Board assigns the responsibility to create and implement an appropriate approach to achieve and assure privacy compliance.

Global Privacy Officer: The role assigned the accountability to co-ordinate and drive the necessary activities to achieve, maintain, develop and report on the implementation of the Privacy Framework. The GPO:

- advises the Executive Board on privacy risks and tolerance;
- reviews privacy related risks; and
- identifies and drives priorities to mitigate identified privacy risks.

The GPO shall also be appointed as the Data Protection Officer for adidas AG and wherever appropriate also for other legal entities within the adidas cooperation unless otherwise required under applicable law.

Privacy Coordinator: The role which is assigned the responsibility to support the Global Privacy Officer coordinating the activities to achieve, maintain, further develop and report on the implementation of the Privacy Framework on a functional, regional or local level.

For the avoidance of doubt: The Privacy Coordinator does not necessarily have to be a designated data protection officer (or similar function), unless explicitly required by applicable law. In that case, the further role description needs to be derived from the relevant laws or regulation.

Privacy Action Owner: The owner of a given business process or task, which needs to be refined, implemented or changed to address a privacy requirement deriving from the Privacy Framework.

Appendix 2: Glossary

Anonymization means to effectively eliminate the link between a distinct natural person on the one hand and the information enclosed in a data record on the other hand to the extent a direct or indirect re-personalization is rendered technically impossible.

Business Process Owner refers to the owner of a business process or task which has to be refined, implemented or changed to address a privacy requirement deriving from the Global Privacy Framework and who has to sign off to risks related to these requirements. The Business Process Owner shall be assigned at the appropriate level of seniority regarding the risk impact involved.

Within a Data Governance Framework, such role would be assigned the title "Data Stewart", if and to the extent the Business Process Owner uses Personal Information for specific purposes without being the Data Owner and therefore serving the Data Owner to achieve/maintain compliance.

Data Custodian refers to a role, which is assigned the oversight and implementation of the technical aspects of data processing and storage through SLAs, quality metrics or other standards without substantial determination of the processing and storage. Such role will mostly be filled by IT functions but can, in cases of shadow IT, also sit with the Business Owner or with third parties, if and to the extent they are committed to the operation and/or hosting of business processes and/or underlying applications, systems or data bases.

Data Owner refers to a role within a data governance framework, which is assigned the accountability for a specific scope of information or data, be it because these data/Information is being initially captured for primary purposes the role owns (e.g. a Head of CRM, if he/she owns the consumer relation) be it because the role is assigned as such data ownership (e.g. a Chief Data Officer as part of a data governance organization).

Data Protection Authority is an administrative and often independent body, which is accountable to oversee the implementation of applicable privacy legislation within a given jurisdiction.

Deletion means to wipe out the link between a data record as well as the information enclosed on the one hand and a distinct natural person on the other hand irrevocably using adequate state of the art technical measures, i.e. by means of anonymization, erasing the whole data record (e.g. through overwriting/reorganization of storage/databases) or by means of destruction or rendering unusable the relevant storage media (including shredding of devices or paper).

Deletion Strategy is a documented set of rules, which outlines the applicable deletion timeline applicable for a dedicated scope of Personal Information within a dedicated scope of processes and underlying applications/systems.

High Risk Processing Activities relate to the processing of Personal Information within business processes, which at least potentially imposes significant Privacy Risks on affected individuals.

Personal Information/Personal Data mean information that can be directly linked to a natural person, regardless how relevant or meaningful the respective information might be from an objective or subjective perspective, including Personal Identifiable Information.

Personal Identifiable Information mean information that, although not immediately linked to a natural person, can be ultimately linked to a natural person, e.g. by means of deduction, merging information from different sources or by means of reverse engineering.

Note: This Privacy Policy applies to Personal Information and Personal Identifiable Information the same way.

Privacy Breach is a relevant threat to the rights and freedoms of an individual comprising of or resulting from (i) the internal treatment of Personal Information by or on behalf of adidas or (ii) an unlawful exposure of Personal Information to Third Parties, e.g. through a cyber-attack or illegal proliferation.

Privacy Commitment: Represents the privacy compliance level the Executive Board has defined for adidas.

Privacy Framework consists of the Fair Play Code of Conduct, this policy, internal standards and guidance documents for key business functions (e.g. Human Resources, Big Data & Data Analytics, Digital Brand Commerce and Global IT) as well as template documents, process blueprints & designs.

Retention refers to a period within which Personal Information must not be deleted but kept for the purpose to fulfil legal obligations or other legitimate purposes, i.e. but not limited to country-specific Tax Laws, Commercial Codes, Stock Cooperation Act, Social Legislation (e.g. commercial transaction logs need to be retained for 6 years under tax law, security log-files shall be stored for 180 days for reverse security investigation purposes).