

Foot Locker Korea Limited Privacy Statement

Foot Locker Korea LLC (“**FOOT LOCKER**” or “**Company**”) establishes and publishes the following Privacy Statement in order to protect personal information and efficiently process any complaints in relation to privacy in accordance with Article 30 of the *Protection of Personal Information Act* (the “**PIPA**”).

1. Collected Personal Information

- a. The personal information collected by FOOT LOCKER at the time of creating your personal account (“**Personal Account**”) is provided below.

When a user signs up for a FOOT LOCKER Personal Account, personal details (e.g., name, date of birth, gender, mobile phone number and email address) used for account verification are required for collection. The user may choose whether to provide profile information e.g., preferred language, additional contact details information, address.

Children’s data privacy: our Services do not target children under the age of 14, and we do not knowingly collect their personal information. If you are concerned about your child’s data privacy, we encourage you to use web-filtering technology to supervise your child’s access to our Services.

- b. When a customer contacts FOOT LOCKER Customer Service, personal details are required for collection (e.g., name, contact details, order information if applicable, content of the query raised). Customer can provide any additional information needed, depending on the type of query raised.
- c. The IP address, cookies, service usage records, device information, and location information may be generated and collected during service use.

A "Cookie" is a small data file that is sent from a webserver to your browser and that is stored on the hard disc of your computer. A cookie contains specific information, for example a unique ID number that keeps track of the webpage(s) visited by you. With this unique number we can keep track of your orders while you shop on our website. In addition, cookies recognize whether you are a registered user, as a result of which we can offer you information that may be important to you in particular.

If you do not register and do not buy anything from us, it is still possible that we save information about you on our website in order to improve our website. Such use, like the number of times that our website is visited and which pages are viewed, cannot be traced back to individual users. This information is only intended for internal use to improve the provision of our services.

Although cookies are accepted and saved automatically by most browsers, you may in general change the settings of your browser in such a manner that this does not happen or does not happen automatically. It may however be that you have to set your browser to accept both (functional) cookies and pop-ups to be able to use all the functionalities of the website, including adding product (s) to your shopping cart and placing an order.

The information collected as described above may or may not be considered “personal information”, depending on whether or not it has a connected to other personal information, etc.

FOOT LOCKER uses the following methods to collect personal information:

- a. Personal information is collected if the user agrees to the collection of personal information and personally enters the information during the process for creating the personal account (on-line or off-line at a FOOT LOCKER store) or during service use.
- b. User’s personal information may be collected via the webpage, email, fax, or phone, during

communications made with customer support.

- c. Personal information may be collected through documents at events or seminars held offline.
- d. Personal information may be obtained from other companies or organizations in partnership with FOOT LOCKER. In such cases, the partnering company will provide the information to FOOT LOCKER after obtaining consent from the user to provide their personal information to FOOT LOCKER, as required by the Personal Information Protection Act.
- e. Generated information, such as device information, may be automatically created and collected during a user access to the PC web or mobile web/app.

2. Processing of Personal Information and Retention Period

FOOT LOCKER processes and holds personal information in accordance with the retention and use period prescribed by the law or such period consented by the data subject.

FOOT LOCKER will obtain separate consent from the user for personal information storage for a specified period for the following purposes.

- a. Subscription to FOOT LOCKER website (the “**Website**”) and management of users: Until the relevant business or group unsubscribes from the Website; provided, however, that the personal information will be kept for further period in the following circumstances:
 - if an investigation or an inquiry is under way in relation to breach of law – until the end of such investigation or inquiry; and
 - if there is any existing claim or debt in relation to the use of the Website – until completion of discharging such claim or debt.
- b. Provision of goods and services: Until completion of the provision of the goods and/or services and payment, subject to any specific requirement under the relevant law.

Relevant statutes, including the Act on the Consumer Protection in Electronic Commerce, etc. and the Protection of Communications Secrets Act, require FOOT LOCKER to store the information for a period of time, as described below. FOOT LOCKER stores the personal information for the period specified by law and in no case shall the information be used for any other purpose.

- c. Under the Act on the Consumer Protection in Electronic Commerce, etc.
 - Records on marks and advertisements: Store for six months
 - Records on Personal Account or withdrawal: Store for five years
 - Records on payment settlements and supply of goods: Store for five years
 - Records on customer complaints or dispute settlements: Store for three years
- d. Under the Protection of Communications Secrets Act
 - Records on sign-in: Store for three months

3. Use of Collected Personal Information

- a. Personal information is used for Personal Account management, such as confirming user intent to sign up, verifying age, verifying the identity of users, identifying users, and confirming user intent to withdraw FOOT LOCKER Personal Account.

- b. In addition to providing existing services, including contents and advertisement, personal information is also used to analyze demographic data, service visitation and usage records, create relationships between users based on their personal information and interests, and provide customized services based on information of friends and areas of interest, in order to discover new service elements to improve upon existing services.
- c. Personal information is used to protect users and provide effective services through diverse means, such as imposing restrictions on service use in violation of laws, regulations, and FOOT LOCKER's Terms of Service, preventing and sanctioning against actions that interfere with seamless service operation, including any unfair service use, preventing account fraud and illegal transactions, providing notices of updates in the Terms of Service, storing records for dispute resolution, and handling civil complaints.
- d. Personal information is used to verify user identity for premium services, process purchases, and payments, and conduct the delivery of products and services.
- e. Personal information is used to provide marketing and promotions through offering information on events and offering opportunities for participation and providing promotional information.
- f. Personal information is used to receive newsletter and marketing communications e.g., about sneaker releases, news, surveys, initiatives and events, to remind you to complete a purchase or a transaction and to send you specific content based of your preferences and interests.
- g. Personal information is used to provide customized services and post advertisements based on the analysis of service usage records and frequency of access, statistics on service use, and other services and statistics.
- h. Personal information is used to create a service environment for users that ensure service use free of any fears that may be associated with security, privacy, and safety.

4. Provision & Entrustment of Personal Information

FOOT LOCKER does not provide personal information to any third party without obtaining consent from the user. However, personal information may be provided, and limited to the instances, which the PIPA permits, including when the data subject consents to the collection of its personal information or there is any statutory requirement to collect personal information.

FOOT LOCKER entrusts part of its operations to third-party businesses in order to provide better services and regulates matters, as well as exercises both management and supervision, necessary to ensure that the entrusted companies safely process personal information in accordance with the Personal Information Protection Act. Unless using services related to affairs that FOOT LOCKER entrusted to consignees, your personal information will not be provided to consignees.

	Entrusted Company	Entrusted Operations
1	Zendesk, Inc.	Customer Service system
2	Intershop communication AG	Webshop service & E-commerce activities
3	Emarsys eMarketing system	Newsletter

FOOT LOCKER may transfer personal information to overseas entities as shown below. (In the case where the transfer is not for the purpose of entrusting the processing of personal information to the recipient, then FOOT LOCKER will seek separate consent from the data subjects).

1	Name of Company	Foot Locker Asia Pte. Ltd.
	Location of Company	410 North Bridge Road, Spaces City Hall, Singapore 188726
	Date of transfer & methods	09/09/2020 & Private cloud hosted solution
	Chief Privacy Officer Contact Information	N/A - In case of questions and/or concerns, please contact privacy@footlocker.com

	Transferred Personal Information List	Personal details (e.g., name, contact details, order information if applicable, content of the query raised). Customer can provide any additional information needed, depending on the type of query raised
	The purpose of the recipient of Personal Information	Customer relations activities Administrative and Technical Support Services E-commerce and Marketing activities
	Personal Information Retention & Usage Period	As per retention period described in this privacy policy
2	Name of Company	Foot Locker Europe B.V.
	Location of Company	Ir. D.S. Tuijnmanweg 3-5, 4131 PN Vianen The Netherlands
	Date of transfer & methods	20/03/2018 & Private cloud hosted solution
	Chief Privacy Officer Contact Information	N/A - In case of questions and/or concerns, please contact privacy@footlocker.com
	Transferred Personal Information List	Personal details (e.g., name, contact details, order information if applicable, content of the query raised). Customer can provide any additional information needed, depending on the type of query raised
	The purpose of the recipient of Personal Information	Customer relations activities Administrative and Technical Support Services E-commerce and Marketing activities
	Personal Information Retention & Usage Period	As per retention period described in this privacy policy

5. Destruction of Personal Information

FOOT LOCKER strictly destroys personal information immediately after the user withdraws account.

However, personal information may be stored safely for a designated period afterward, if FOOT LOCKER obtains separate consent from the user to store the personal information for a certain period, or if FOOT LOCKER is required by law to store the information for a specified period.

Personal information is immediately destroyed to an un-restorable state once the purpose of collecting and storing personal information is fully served, which includes the user's account cancellation, service termination, and/or expiration of the personal information storage period that was approved by the user.

Personal information stored under the law is immediately destroyed to an un-restorable state once the storage period is expired.

Personal information stored in electronic form is safely deleted using a technical approach to prevent it from being restored or regenerated while written information is shredded or incinerated.

6. Rights of Users & Legal Representatives and Exercising Those Rights

Users can log into his/her FOOT LOCKER Personal Account and go to "Account Overview" to view or update their personal information at any time.

Users can go to service@footlockerkorea.kr to exercise their statutory rights including browsing, modifying, deleting, and requesting for ceasing of processing, their personal information at any time.

Where a user requests the correction of errors in his/her personal information, the relevant personal information will not be used or provided until the correction is made. If any incorrect personal information has already been provided to a third party, the corrected information will be immediately notified to the third party without delay so as to ensure that the necessary correction is made.

7. Action Taken to Protect Personal Information

Personal information is being encrypted.

Passwords, unique identifiable information, account numbers, and credit card numbers are encrypted for storage as required by law. Email addresses and mobile phone numbers are also encrypted and stored.

Foot Locker has implemented specific security measures for the protection against loss, abuse or the adjustment of information provided by you. All personal data, including credit card numbers sent over the Internet are encrypted with the use of SSL (Secure Socket Layer), Secure Server Certification Authority RSA Data Security Inc. US and a VeriSign SSL, by which transactions performed via the internet are secured. VeriSign, Inc. is a leading provider of Public Key Infrastructure and digital certification solutions used by many companies, websites and consumers to exchange information over the internet and private networks in a safe manner.

The browsers that support placing orders with the use of SSL /TLS Technology include Google Chrome 51 and higher; Microsoft Internet Explorer 11 and higher; Mozilla Firefox 47 client for PCs; and the Safari 9.1 client for Macs; Mobile Safari and Google Chrome for mobile. If you use an older version of these browsers or another browser which does not support the performance of secured transactions or if your computer forms part of a LAN (local area network) on which a firewall is installed which prevents the performance of secured transactions, you cannot perform secured transactions. If this is the case, we kindly ask that you choose one of the offline methods of payment to place your order.

If you make use of our website, you are responsible for keeping your profile and password confidential and for limiting access to your computer to prevent the unauthorized access to your profile. You accept that you are responsible for all the activities that take place in your profile or with the use of your password.

Personal information is safely protected from internal and external security threats.

To prevent user's personal information from being leaked or damaged through acts of hacking or computer viruses, the system of FOOT LOCKER is installed in controlled areas that cannot be accessed externally. Personal information is backed-up on a regular basis as preemptive measures against potential damage to personal information, while the latest vaccine programs are used to prevent such leakage or damage. Encoded communication is also used to transfer personal information safely via networks.

Foot Locker has implemented the appropriate physical, administrative, and technical security measures to protect against unlawful access, loss, misuse or alteration of the information you provide. When we collect data through the site, we encrypt your personal information, including your credit card number, when transmitting over the Internet using encryption technology Secure Socket Layer (SSL) coding, to safeguard your Internet transactions. You are strongly recommended not to send full credit or debit card details in unencrypted electronic communications with us. We maintain physical, electronic and procedural safeguards in connection with the collection, storage and disclosure of your information. Our security procedures mean that we may occasionally request proof of identity before we disclose personal information to you. You are responsible for protecting against unauthorised access to your password and to your computer.

Employees that handle personal information are kept to a minimum.

Employees that handle personal information kept to a minimum and the work PCs of employees permitted to view personal information from the personal information processing system do so only via a secure connection and via approved devices, reducing the leakage risk of personal information. FOOT LOCKER continuously stresses that protecting personal information is its utmost priority by training employees who handle personal information on a regular basis while also frequently holding training sessions and campaigns for the entire FOOT LOCKER staff.

8. Chief Privacy Officer & Responsible Personnel

FOOT LOCKER has designated the following persons as the Chief Privacy Officer and Personal Information Management Team. They remain responsible for responding to FOOT LOCKER user inquiries regarding personal information and resolving any related complaints.

Chief Privacy Officer:

Name: Ivar Oosterveld

Position: VP Legal

Email: Ivar.Oosterveld@footlocker.com and privacy@footlocker.com

Contact the organizations shown below to file reports or seek consultation for other privacy infringements.

- a. Privacy Infringement Report Center (privacy.kisa.or.kr / Phone no. 118)
- b. Cyber Crime Investigation Unit, Supreme Prosecutor's Office (www.spo.go.kr / Phone no. 1301)
- c. Cyber Terror Response Center, National Police Agency (police.go.kr / Phone no. 182)

9. Obligation to Notify Prior to Amendment

Users will be notified of any addition, deletion, and/or modification in this Privacy Statement through notification at least seven (7) days prior to the scheduled amendment.

However, notifications for amendments that affect significant rights of users, including changes to the collected personal information or to the purpose of using such information, will be filed at least thirty (30) days prior to the scheduled amendment. In such cases, the consent of users may be obtained once more upon necessity.

Notification date: 15 February, 2021

Effective date: 22 February, 2021

The previous versions of this Privacy Statement can be found below:

Not applicable