BHARAT FORGE | KALYANI

Data Protection and Privacy Policy

Name of the Document	Data Protection and Privacy Policy
Version	2
Issuing Authority / Document owner	Human Resources
Last Revision Date	01.07.2021

1. Introduction

Data Protection policy of Bharat Forge Limited (BFL) indicates that we are dedicated to and responsible for processing the information of our, customers, stakeholders, employees and other interested parties with absolute caution and confidentiality.

This policy describes how we collect, store, handle and secure our data fairly, transparently, and with confidentiality.

2. Scope

This policy applies to employees, contractors, consultants, vendors, customers and clients and business partners who receive personal information from BFL, who have access to personal information collected or processed by BFL, or who provide information to BFL, regardless of geographic location. All employees of BFL are expected to support the privacy policy and principles when they collect and / or handle personal information, or are involved in the process of maintaining or disposing of personal information.

3. Policy Elements

As a key part of our operations, we gather and process any information or data that makes an individual identifiable such as full name, physical address, email address, photographs, etc. This information is collected only with the full cooperation and knowledge of interested parties. Once this information is available to us, the following rules apply to our company.

Our data will:

a. Be precise and consistently updated;
b. Is collected legitimately and with a clearly stated purpose;
c. Be processed by the company in line with its legal and ethical binds;
d. Have protection measure that protects it from any unauthorized or illegal access occurring by internal or external parties.

Our data will NOT:

a. Be communicated informally;
b. Exceed the specified amount of time stored;
c. Be transferred to organizations, states or countries that do not acquire proper data protection policies;
d. Be spread to any party unless approved by the data's owner (except for the legitimate requests demanded from law enforcement authorities).

4. Roles and Responsibilities

Everyone who works for or with BFL is responsible for ensuring that the collection, storage, handling, and protection of data is being done appropriately.

General guidelines

a. Access to data covered by this policy is restricted only to those who need it for their work;
b. Data is not to be shared informally. When access to confidential information is required, employees request it from their line managers;

c. We provide comprehensive training to all employees to help them understand their responsibilities when handling data;
d. Employees keep all data secure, by taking sensible precautions and following the Data Storage guidelines specified below;
e. In particular, strong passwords are used and never shared;
f. Personal data is not disclosed to unauthorized people, within the company or externally;
g. Employees request help from their line manager or the data protection officer when they are unsure about any aspect of data protection;

In addition, the following functions within BFL hold the key areas of responsibility:

i. **Information Security Manager** is responsible for:

a. Providing oversight and continuous enhancement of cyber security and in risk management awareness programs and improvements;
b. leading the design, implementation, operation and maintenance of the Information Security Management System;
c. Ensuring periodic testing is conducted to evaluate the security posture of the Information Security by conducting periodic reviews of BFL to ensure compliance with the System Security Plans;
d. Leading the design and operation of related compliance monitoring and improvement activities to ensure compliance with both internal security policies, and applicable laws and regulations;
e. Developing and managing controls to ensure compliance with the wide variety and ever-changing requirements resulting from standards and regulations.

ii. IT Systems Administrator responsible for:

a. Ensuring that access to personal data of users registered on the BFL Website is restricted only to authorized personnel;
b. Ensuring that access to the personal data of users registered on the BFL website will not be shared with or provided to unauthorized personnel

iii. **Commercial Department is responsible for:**

a. Ensuring that access of personal data is only to authorized personnel. The department will maintain the data at designated servers location of BFL server with restricted access of authorised personnel as per internal define process;

b. Ensuring that the access of the personal data will not be shared with or provided to unauthorized personnel;

5. Collection and use/process of Personal Data

Personal Data refers to data that lets BFL, know the specifics of the individual and which may be used to identify, contact or locate the individual.

We collect and use the personal data for one or more these reasons:
a. When it is in our legitimate interests which are our business or commercial reasons for using personal data;
b. Administering relationships services;
c. To fulfill contractual obligations;

d. Conducting market or customer satisfaction research;
e. Providing individuals with information concerning products and services which we believe will be of interest;
f. Compliance with any requirement of law, regulation, associations, voluntary codes we decide to adopt;
g. For the purpose of, or in connection with, any legal proceedings (including Prospective legal proceedings), for obtaining legal advice or for establishing, exercising or defending legal rights.

6. Rights relating to Personal Data

a. Any individual whose personal data is collected by BFL may request the information regarding his personal data, how the data was collected and for what purpose.
b. If the personal data collected is incorrect or incomplete, the individual may demand to get it corrected or added.
c. Any individual whose personal data is collected may direct to erase the personal data collected if such data as collected has no legal basis or the legal basis has ceased to apply. When BFL receives the request for deletion of personal data, it shall intimate regarding the deletion of the same or the reason why it cannot be deleted.
d. Any individual whose personal data is collected may request to stop processing the data. Upon receiving the request BFL shall inform the individual if it has legitimate grounds to process your data. Even after someone exercises right to object, BFL may continue to hold the data to comply with any regulatory requirements.
e. Any individual may request for withdrawal of his/her consent for processing of data for which earlier consent was ought to be taken.

7. Data Storage

These rules describe how and where data are safely stored. When data is **stored on paper,** it is kept in a secure place accessed only by authorized personnel.

These guidelines also apply to data that is usually stored electronically but has been printed out for certain reasons:

a. The paper or files are kept in a locked drawer or filing cabinet;
b. Employees make sure paper and printouts are not left unattended;
c. Data printouts are securely shredded and disposed when no longer needed.

When data is **stored electronically**, it must be protected from unauthorized access, accidental deletion and malicious internal or external threats.

a. Data should be protected by strong passwords that are updated regularly and never shared among employees;
b. If data is stored on removable media (like a CD or DVD, External HDD, etc.), these should be kept locked away securely when not being used;
c. BFL Network of computers is restricted from using or transferring any data via a CD, DVD, USB, and External HDD, unless authorized for specific personnel with additional privileges;
d. Data should only be stored on designated servers, and should only be uploaded on to approved cloud computing services;
e. Secure communication is empowered with TLS (Transport Layer Security);
f. Servers containing personal data are sited at secure locations, where access is restricted for authorized personnel only and monitored;

g. Data is backed up daily. Backups are tested regularly, in line with the company's standard backup procedures;
h. All servers and computers containing data are protected by the monitoring system and the firewall system;
i. All data entering into BFL systems and website are stored as associated with a specific user account to and measures to prevent privilege escalation are always in place;
j. All personal data entering into the database of the BFL website are protected with certificates that ensure encrypted communication when receiving and sending information is being used.

8. Data Protection actions

To exercise data protection, BFL takes reasonable steps and is committed to:
a. Restrict and monitor access to sensitive data, and keep it in as few places as possible;
b. Establish effective data collection procedures;
c. Provide employees with online privacy and security measures training;
d. Build secure network to protect online data from cyber-attacks;
e. Establish clear procedures for reporting privacy breaches or data misuse;
f. Include contract clauses or communicate statements on how we handle data;
g. Update the data continuously and as mistakes are discovered;
h. Install tracking logs to monitor employee's activities ensuring data is not being misused;
i. Install firewall and protection software that prevents employees to share and distribute data from BFL devices externally, by detecting when a large amount of data is being transferred either through email, or via external drives;
j. Establish data protection practices (document shredding, secure locks, data encryption, frequent backups, access authorization etc.).

9. Collection of personal data

BFL shall obtain consent in writing from the provider of sensitive personal data regarding purpose of usage before collecting such information.

10. Disclosure of personal data

BFL shall not disclose any sensitive personal data or information to any third party without obtaining prior permission from the provider of such information unless such information is being shared with a Government Agency mandated under law where BFL has received written request from such Government Agency.

The personal data may be disclosed to BFL management, auditors, service providers, regulators, governmental or law enforcement agencies or any person, BFL reasonably thinks necessary for the processing purposes.

If BFL undertakes transactions that involves the disclosure of personal data on behalf of a counterparty, it shall be the responsibility of such to ensure that it has all necessary rights to permit us to process and disclose the personal data accordingly.

In some circumstances, if the personal data is shared with external parties, the same shall be informed to the concerned individual. Individuals also have a right to object to sharing/processing of their personal data which can be done through email to HR Department. In case of employee's objections repercussion shall be communicated appropriately.

11. Monitoring of electronic records

To the extent permitted by applicable law, we may record and monitor electronic communications to ensure compliance with our legal and regulatory obligations and internal policies and for the purposes outlined above.

12. Amendment in personal data provided

Individuals about whom we process personal data may request a copy of the personal data held in relation to them by us. If any personal data is found to be wrong, the individual concerned has the right to ask us to amend, update or delete it, as appropriate.

13. Duration of Storage

We retain personal information for as long as we reasonably require it for legal or business purposes. In determining data retention periods BFL takes into consideration local laws, contractual obligations, and the expectation and requirements of our customers. When we no longer need personal data, we securely delete or destroy it.

14. Confidentiality of processing

Personal data is subject to data secrecy. Any unauthorized collection, processing, or use of such data by employees is prohibited. Any data processing undertaken by an employee that he/she has not been authorized to carry out as part of his/her legitimate duties is unauthorized. The "need to know" principles applies. Employee may have access to personal information only as is appropriate for the type and scope of the task in question. This requires careful breakdown and separation, as well as implementation of roles and responsibilities.
Employees are forbidden to use personal data for private or commercial purposes, to disclose it to unauthorized persons, or to make available in any other way. HR/Supervisors must inform the employees

at the start of the employment relationship about the obligation to protect data secrecy. This obligation shall remain in force even after employment has ended.

15. Children

BFL shall not knowingly collect personal data from children without insisting that they seek prior parental consent if required by applicable law. We will only use or disclose personal data about a child to the extent permitted by law, to seek parental consent pursuant to local law and regulations or to protect a child. The definition of "child" or "children" should take into account applicable laws as well as national and regional cultural customs.

16. **Non-personal data collected automatically**

When you access our website, we may automatically (i.e. not by registration) collect non-personal data (e.g. type of Internet browser and operating system used, domain name of the website form which you came, number of visits, average time spent on the site, pages viewed). We may use this data and share it with our affiliates to monitor attractiveness of our website and improve their performance or content.

17. Link to other websites

BFL may contain links to other websites. BFL is not responsible for the privacy practices or the content of other websites as such websites are not under the control of BFL.

18. Violation categorization

Violations are categorized into three levels namely: Low, Medium and High severity. These will be applicable as and when breach of any policy is identified and the cause is ascertained. Any other violations if not explicitly mentioned shall be subject to disciplinary action based on the business impact and potential loss to the organization.

Sr. No	Type of Violation	Severity		
	Physical Security	**High**	**Medium**	**Low**
1	Unauthorized entry into restricted areas			☐
2	Allowing unauthorized entry into restricted areas			☐
3	Entry into premises without identification card			☐
4	User not wearing Physical Access card			☐
5	Bringing Unauthorized storage devices (USB, CD, tapes, etc.)		☐	
6	Unauthorized removal of equipment from the premises		☐	
7	Unauthorized relocation of equipment inside the premises		☐	
8	Leaving laptops in insecure areas (i.e., unlocked cabinets)			☐
9	Non-adherence to environmental precautions for Data Centre & Server room			☐

Sr. No	Type of Violation	Severity		
	Email Security			
10	Unauthorized use of another person's e-mail		☐	
11	Intentionally sending viruses through e-mail attachments	☐		

12	Transmitting confidential or sensitive company informationwithout sufficient security	?		
13	Inappropriate auto forwarding of email			?
14	Using e-mail in a manner that: • interferes with normal business activities or hampersemployee productivity, • embarrassment • consumes more resources • involves solicitation • is associated with any for profit outside businessactivity		?	
15	Blanket forwarding of e-mail			?
16	Sending obscene or derogatory e-mails		?	
	Password Policy			
17	Password sharing / disclosure		?	
18	Insecure conveyance / storage of passwords by normal users		?	
19	Insecure conveyance / storage of critical passwords		?	
20	Making unauthorized password resets of other users in theirabsence		?	
21	Making password resets of other users in their absence for emergency business purposes			
22	Not disabling default passwords		?	
23	Unauthorized logical access to systems inconsistent with one'sjob responsibilities		?	
24	Setting up unauthorized wireless access points	?		
25	Use of systems inconsistent with one's job responsibilities		??	
	Software Compliance			
26	Use of unapproved software		?	
27	Use of software using alternatives after expiry		?	
28	Providing and installing software without IT HOD approval		?	
29	Downloading software without IT HOD approval		?	
	USB			
30	Use of personal/unapproved USB storage devices		?	
31	Use of unauthorized USB storage device		?	
32	Providing USB access without approval		?	

Sr. No	Type of Violation	Severity		
	Internet Security			
33	Violation of Internet Usage policy		?	
34	Providing internet access without approval		?	
	Social Media			

35	Posting BFL Proprietary, Confidential and sensitive information on social media without approval		?	
	Data Leakage			
36	Connecting personal devices in BFL environment		?	
37	Unauthorized copying or disclosure of sensitive/confidentialinformation, in any form, either due to gross negligence or otherwise.	?		
	Endpoint Security			
38	Ignoring any Malware suspect notification			?
39	Disable of Security controls such as Antivirus, Patch Management, etc.		?	
	Data Centre / Server Room			
40	Unauthorized access to Data centre / Server room	?		
41	Non -adherence to environmental precautions for Data Centre / Server room		?	
42	Providing administrative unauthorized logical access (Abuse of privileges)	?		
43	Firewall rule created without any approval	?		
44	Providing any firewall rule without IT manager approval		?	
45	Hosting of any application/website on internet without following web hosting procedure		?	
46	Connecting any external network without approval from IT Manager		?	
47	Unauthorized changes to information, applications, systems, hardware		?	
	Personal Records, Data			
48	Forgery or alteration of any document/data in the system, files	?		
49	Unauthorized alteration or Manipulation of files	?		
50	Fraudulent financial reporting	?		
51	Falsification/Destruction of company records	?		
52	Disclosure of confidential data	?		

19. **Questions and Comments**

BFL will respond to reasonable requests to review your personal data and to correct, amend or delete any inaccuracies. If you have any questions or comments about the BFL Data Protection Policy (e.g. to review and update your personal data) you may contact to Information Security Manager.
The contact person responsible for managing the Data Protection process is:

Person: **Information Security Manager**
Name: **Mr. Mahesh Wagh**
Email: **Mahesh.Wagh@kalyanitechnologies.com**
Phone: **020 6704 2938**

20. Grievance/ Complaints

Enforcement of this policy is mandatory & violations of this policy shall be reported to HR Department. An Individual can lodge a complaint over our processing of his/her personal data address to HR Department at email id: JitendraYerudkar@bharatforge.com

21. Disciplinary actions

The HR Department shall act on any and all complaints received under this policy or act *suo motu* to investigate any violations of this policy. Any violations of this policy may lead to disciplinary actions (as per the table below) which will be determined based on the nature and factors of violation on a case to case basis as per the violation categories in Point 27 above.

Severity	Disciplinary Action
Low	1. Verbal Warning (Manager/HR) 2. Written Warning from HR
Repetitive Low	Final Warning letter from HR
Medium	Counselling and Final Warnings letter from HR
Repetitive Medium	Termination
	Legal and Police Action if required
High	Termination Legal and Police Action if required

The whistle-blowers will be protected from any intimidation, victimization or discrimination for bringing a complaint under this Policy or taking part in any investigation unless they have acted in bad faith or have made untrue statements. Any retaliation against a whistle-blower for bringing a complaint will be treated as a disciplinary offence.

22. Changes

We recognize that data protection and privacy is an ongoing responsibility, so we reserve our right to make changes to this Data Protection and Privacy Policy from time-to-time as we undertake new personal data practices or adopt new privacy policies, etc.