



## **PIMS ISO-27701 Compliance**

### **Privacy Policy**

## **National Pension and Provident Fund (NPPF)**



<b>Code:</b>	<i>PIMS ISO –PP</i>
<b>Distribution List:</b>	
<b>Confidentiality level:</b>	<b>Confidential</b>

**Version control**

Version	Date	Created by	Short description of modification
1.0	22 <sup>nd</sup> May 2023	Qadit System and Solutions Pvt.Ltd	Privacy Policy for PIMS ISO 27701

**Review and Approval**

Review / Approval Date	Approver	Review / Approval Notes
20 <sup>th</sup> July 2023	Mr. Dorji Penjor (CEO) Mr. Tshen Norbu (Operations Director) Mr. Phurpa Thienley (Investment Director) Mr. Kinzang Wangdi (Chief ICT) Mr. Tashi Dhendup (Assistant Manager, Admin) Mr. Changa Dawa (Assistant Manager, LSD) Mrs. Kezang Choden (ISM/DPO)	Approved

*The information contained within this document is the property of National Pension and Provident Fund, Bhutan and is issued in confidence and must not be reproduced in whole or in part or used in tendering or manufacturing purpose or given or communicated to any third party.*



## **Table of Contents**

<b>1.</b>	<b>Privacy Policy / Notice.....</b>	<b>4</b>
1.1	Introduction .....	4
1.2	Information That We Collect .....	4
1.3	How We Use Your Personal Data .....	5
1.4	Your Rights .....	5
1.5	Sharing and Disclosing Your Personal Information .....	6
1.6	Safeguarding Measures .....	6
1.7	Consequences of Not Providing Your Data.....	7
1.8	Legitimate Interests .....	7
1.9	Cookie Notice .....	7
1.10	Minors and Children’s Privacy .....	8
1.11	How Long We Keep Your Data .....	8
1.12	How to Contact Us.....	8
1.13	Consent (Physical Hard Copy) .....	9
1.14	Consent (Digital Format) .....	9
1.15	Grievance Officer.....	9
<b>2.</b>	<b>Internal Guidelines .....</b>	<b>9</b>
2.1	Privacy Notice vs Privacy Policy.....	9
2.2	Privacy Notice – When and How? .....	10
2.3	Double Opt-in Method .....	10



## **1. Privacy Policy / Notice**

### **1.1 Introduction**

**National Pension and Provident Fund (Herewith referred to as NPPF)** (*'we' or 'us' or 'our'*) gathers and processes your personal information in accordance with this privacy notice and in compliance with the relevant data protection regulation and laws. This notice provides you with the necessary information regarding your rights and our obligations, and explains how, why and when we process your personal data.

**National Pension and Provident Fund (NPPF)** registered office is at Samtem Lam, Thimphu Bhutan and we are a company registered in Bhutan. We act as the **PII Controller** when processing your data.

### **1.2 Information That We Collect**

**National Pension and Provident Fund (Herewith referred to as NPPF)** processes your personal information (information that specifically identifies an individual or that is linked to information that identifies a specific individual) to meet our legal, statutory and contractual obligations and to provide you with our products and services. We will never collect any unnecessary personal data from you and do not process your information in any way, other than as specified in this notice.

***The personal data that we collect are:***

- names
- date of births
- national id number
- phone numbers
- email addresses
- mailing addresses
- job titles
- usernames
- payment details
- Leave/ Studies details
- Organization you work
- Spousal details
- Children details
- Nomination information

By accessing our website or providing data directly to NPPF through customer website/ portal or through NPPF internal portal/ any other source, you agree and consent to the collection and use of



your personal information and sensitive personal information for specific verification and screening purposes only.

***We collect information in the below ways:***

- Online job application form under career option on NPPF's website
- **NPPF** prospective customers provides their name, email id and contact information on the contact us form on NPPF's website. Please review each NPPF's terms of use and privacy policies carefully before using the services.
- Customers who uses our services based on the contract entered, shares any kind of personal data that is required to perform the Employee background and credentials verification.
- Information from other sources (We may obtain information, including Personal Data, from third parties and sources other than the Service, such as our partners, mutual connections, advertisers, credit rating agencies, and Integrated Services. If we combine or associate information from other sources with Personal Data that we collect through the Service, we will treat the combined information as Personal Data in accordance with this Policy

### **1.3 How We Use Your Personal Data**

NPPF takes your privacy very seriously and will never disclose, share or sell your data without your consent, unless required to do so by law. We only retain your data for as long as is necessary and for the purpose(s) specified in this notice. Where you have consented to us providing you with promotional offers and marketing, you are free to withdraw this consent at any time. ***The purposes and reasons for processing your personal data are detailed below:***

- *We collect your personal data in the performance of a contract or to provide a service. We use the information to operate, maintain, enhance and provide service, to provide the services and information that you request, to respond to comments and questions and to provide support to users of the Service. We process personal data collected in performance of a contract solely in accordance with the directions provided by the contract.*
- *We may use your email address or other information to contact you for administrative purposes such as customer service, to address intellectual property infringement, right of privacy violations or defamation issues related to personal data posted on the Service*

### **1.4 Your Rights**

You have the right to access any personal information that NPPF processes about you and to request information about:

- What personal data we hold about you
- The purposes of the processing
- The categories of personal data concerned
- The recipients to whom the personal data has/will be disclosed



- How long we intend to store your personal data for
- If we did not collect the data directly from you, information about the source

If you believe that we hold any incomplete or inaccurate data about you, you have the right to ask us to correct and/or complete the information and we will strive to do so as quickly as possible; unless there is a valid reason for not doing so, at which point you will be notified.

You also have the right to request erasure of your personal data or to restrict processing in accordance with the data protection laws; as well as to object to any direct marketing from us. Where applicable, you have the right to data portability of your information and the right to be informed about any automated decision-making we may use.

If we receive a request from you to exercise any of the above rights, we may ask you to verify your identity before acting on the request; this is to ensure that your data is protected and kept secure. Requests to access, change, or remove your information will be handled within thirty (30) days.

## **1.5 Sharing and Disclosing Your Personal Information**

We do not share or disclose any of your personal information without your consent, other than for the purposes specified in this notice or where there is a legal requirement.

### **A. Unrestricted information**

Any information that you voluntarily choose to include in a Public Area of the Service, such as a public profile page, will be available to any Visitor or User who has access to that content.

## **1.6 Safeguarding Measures**

NPPF takes your privacy seriously and takes every reasonable measure and precaution to protect and secure your personal data. We work hard to protect you and your information from unauthorised access, alteration, disclosure or destruction and have several layers of security measures in place, **including:**

- Encryption of data during transit (HTTPS)
- Encryption of data at rest
- Restricted access to only authorized personnel through authentication and password mechanisms
- Implementation of anti-malware software
- Network protection through firewalls



However, no method of transmission over the Internet, or method of electronic storage, is 100% secure. We cannot ensure or warrant the security of any information you transmit to us or store on the Service, and you do so at your own risk. We also cannot guarantee that such information may not be accessed, disclosed, altered, or destroyed by breach of any of our physical, technical, or managerial safeguards. If you believe your Personal Data has been compromised, please contact us as set forth in the “Contact Us” section.

Our security management standards are in compliance with ISO 27001:2013 and ISO 9001:2015 which is a widely recognized international security management standard that specifies security management best practices and comprehensive security controls, by way of which we also meet the requirements of reasonable security practices under the Information Technology Act, 2000. Our compliance with ISO 27001 demonstrates our commitment to information security at every level.

If we learn of a security systems breach, we will inform you of the occurrence of the breach in accordance with applicable law.

### **1.7 Consequences of Not Providing Your Data**

You are not obligated to provide your personal information to NPPF, however, as this information is required for us to provide you with our services, we will not be able to offer some/all our services without it.

### **1.8 Legitimate Interests**

As noted in the ‘*How We Use Your Personal Data*’ section of this notice, we occasionally process your personal information under the legitimate interests’ legal basis. Where this is the case, we have carried out a thorough Legitimate Interests’ Assessment (LIA) to ensure that we have weighed your interests and any risk posed to you against our own interests; ensuring that they are proportionate and appropriate.

We use the legitimate interests’ legal basis for processing direct marketing emailers / phone calls and have identified that our interests are to provide you with high quality, best in industry, performance support system to ease and improve user onboarding, support and training.

### **1.9 Cookie Notice**

A ‘**cookie**’ is a small piece of data sent from a website and stored on the user’s computer by the user’s web browser while the user is browsing. When you visit a site that uses cookies for the first time, a cookie is downloaded onto your computer/mobile device so that the next time you visit that site, your device will remember useful information such as visited pages or logging in options.

Cookies are widely used in order to make websites work, or to work more efficiently, and our site relies on cookies to optimize user experience and for features and services to function properly.



We use automatically collected information and other information collected through our website through cookies and similar technologies to: (i) personalize our service, such as remembering your information so that you will not have to re-enter it during a visit or on subsequent visits; (ii) provide customized advertisements, content, and information; (iii) monitor and analyze the effectiveness of Service and third-party marketing activities; (iv) monitor aggregate site usage metrics such as total number of visitors and pages viewed; and (v) track your entries, submissions, and status in any promotions or other activities on the Service.

These cookies do not collect personal information about you. A persistent cookie remains on your hard drive after you close your browser so that it can be used by your browser on subsequent visits to the Service. Persistent cookies can be removed by following your web browser's directions. A session cookie is temporary and disappears after you close your browser. You can reset your web browser to refuse all cookies or to indicate when a cookie is being sent. However, some features of the Service may not function properly if the ability to accept cookies is disabled.

Most web browsers allow some control to restrict or block cookies through the browser settings, however if you disable cookies you may find this affects your ability to use certain parts of our website or services.

### **1.10 Minors and Children's Privacy**

Protecting the privacy of young children is especially important. Our Service is not directed to children under the age of 16, and we do not knowingly collect Personal Data from children under the age of 16 without obtaining parental consent. If you are under 16 years of age, then please do not use or access the Service at any time or in any manner. If we learn that Personal Data has been collected on the Service from persons under 16 years of age and without verifiable parental consent, then we will take the appropriate steps to delete this information. If you are a parent or guardian and discover that your child under 16 years of age has obtained an Account on the Service, then you may alert us at [kezang.choden@nppf.org.bt](mailto:kezang.choden@nppf.org.bt) and request that we delete that child's Personal Data from our systems.

### **1.11 How Long We Keep Your Data**

**NPPF** only ever retains personal information for as long as is necessary to fulfill the purposes outlined in this Privacy Policy, unless a longer retention period is required or permitted by law (such as tax, accounting or other legal requirements) and we have strict review and retention policies in place to meet these obligations. Where you have consented to us using your details for direct marketing, we will keep such data until you notify us otherwise and/or withdraw your consent.

### **1.12 How to Contact Us**

**NPPF** only processes your personal information in compliance with this privacy notice and in accordance with the relevant data protection laws. If, however you wish to raise a complaint regarding





the processing of your personal data or are unsatisfied with how we have handled your information, you have the right to lodge a complaint with our Data Protection Officer at [kezang.choden@nppf.org.bt](mailto:kezang.choden@nppf.org.bt)

### **1.13 Consent (Physical Hard Copy)**

**NPPF** takes your privacy seriously and will only process your personal data with your consent and in accordance with the terms stated in our Privacy Notice. If you consent to us collecting and processing your personal data, please sign below:

I, \_\_\_\_\_, (PII Principal's name) confirm that I have been provided with a copy of **NPPF**'s Privacy Notice & Terms & Conditions prior to giving consent.

**Signature:** \_\_\_\_\_ **Name:** \_\_\_\_\_  
**Time:** \_\_\_\_\_ **Date:** \_\_\_\_\_

### **1.14 Consent (Digital Format)**

**NPPF** takes your privacy seriously and will only process your personal data with your consent and in accordance with the terms stated in our Privacy Notice. If you consent to us collecting and processing your personal data, please tick the check-box below:

I, \_\_\_\_\_, ( PII Principal's name) consent to you processing my personal data as detailed in your Privacy Notice:

### **1.15 Grievance Officer**

**NPPF** has appointed Mrs. Kezang Choden as the Data Protection Officer/Grievance Officer. She can be reached at [kezang.choden@nppf.org.bt](mailto:kezang.choden@nppf.org.bt). If there is a breach/incident found related to data privacy, an email can be shared to the Chief Privacy Officer/Grievance Officer in the above set email id. The timeline to attend to resolving minor incidents (incidents which do not cause no/very negligible damage) would be next 24 hours. With respect to other major/critical incidents – first level would be attended to in the next 24 hours and subsequently would be resolved within a maximum timeline of 72 hours depending on the gravity of the issue.

If you have any queries, kindly contact us at [kezang.choden@nppf.org.bt](mailto:kezang.choden@nppf.org.bt) We will employ all commercially reasonable efforts to address the same.

## **2. Internal Guidelines**

### **2.1 Privacy Notice vs Privacy Policy**

The two terms are used interchangeably, and there is no universally defined difference. However, some definitions suggest a Privacy Notice is the content presented at the time personal data is  
Confidentiality Level: **Internal**



obtained (pop-up, on-screen, paper form etc); whereas the Privacy Policy is a constant poster, website page, link that is always available for visitors/individual to read – both having the same content.

## **2.2 Privacy Notice – When and How?**

A privacy notice shall be provided to ALL individuals when NPPF processes their personal data, but the context/content of the notice will vary depending on the legal basis the processing happens. If consent is being used as a lawful basis for processing, the consent section must be kept at the end of the form for each data subject, with an unticked, opt-in box or affirmative action mechanism for each processing activity.

## **2.3 Double Opt-in Method**

A double-opt in method can also be used whereby the data subject consents via tick box, then has to follow an email link to make sure that it is the correct person consenting – this double opt-in can also serve as evidence of the consent and must be retained.