

**Privacy Notice for  
ING Hubs PH employees**  
(v4.0)

## Contents

1. Purpose and scope of this Privacy Notice.....	3
2. The types of personal data we process.....	4
3. What we do with your personal data .....	6
4. Who we share your data with and why .....	9
5. Your rights and how we respect them .....	11
6. Your duty to provide data.....	133
7. How we protect your personal data.....	14
8. Changes to this Privacy Notice.....	14
9. Contact and questions.....	14

ING Bank N.V. is a European financial institution and is subject to the data protection obligations set out in the EU General Data Protection Regulation 2016/679 ('GDPR'). To comply with GDPR, we have implemented data protection principles on a global scale, through our Global Data Protection Policy ('GDPP'). The GDPP is binding on all ING entities, subsidiaries, branches, representative offices, and affiliates worldwide and approved by the EU data protection authorities. Therefore, in addition to local privacy laws and regulations, ING Bank N.V. has resolved that all its entities, subsidiaries, branches, representative offices, and affiliates worldwide will comply with the GDPP, regardless of geographical location of employees or trainees.

ING Hubs B.V. Philippine Branch ('ING Hubs PH') is the Philippine branch office of ING Hubs B.V., which is in turn a wholly owned subsidiary of ING Bank N.V. ING Hubs PH operates within the ING Bank governance. ING Hubs PH and support function charters, organisational charts, key committee mandates, ING Hubs PH policies, and internal control framework governance follow the ING Bank Policies.

Under the Data Privacy Act of 2012 (Republic Act No. 10173) (the 'DPA'), consent of the data subject is required for processing personal data and sensitive personal data, subject to limited exceptions under the DPA and other applicable laws and regulations. As such, we require you to read this Privacy Notice for ING Hubs PH employees carefully and to confirm that you agree.

If we need to process the personal data of your dependent(s) and/or your emergency contact person(s) to fulfil obligations under or in relation to your employment contract or to manage our employment relationship, or if we are legally allowed or authorized to do so under local law, you guarantee that you are specifically authorized by such dependent(s) and/or emergency contact person(s) to provide such information to us.

This is the Privacy Notice for employees of ING Hubs B.V. Philippine Branch ('ING Hubs PH', 'we', 'us' and 'our'), and it applies to us as long as we process personal data that belongs to individuals ('you').

This Privacy Notice supplements the ING Bank N.V. Privacy Statement for Employees which can be accessed by visiting this link: [ING Bank N.V. Privacy Statement for Employees](#).

## 1. Purpose and scope of this Privacy Notice.

At ING Hubs PH, we understand that your personal data is important to you. This Privacy Notice explains in a simple and transparent way what personal data we collect, record, store, use and process and how. Our approach can be summarised as: the right people use the right data for the right purpose.

This Privacy Notice applies to

- all past and present employees, including trainees, of ING Hubs PH in relation to data processed by ING Hubs PH in connection with their employment or training agreement ('you').

This Privacy Notice does not apply to

- Independent contractors or anyone else hired to work at ING Hubs PH on anything other than on the basis of an employment contract. *Please refer to the 'Privacy Notice for ING Hubs PH supplier personnel'.*
- Job applicants. *Please refer to the separate document 'Privacy Notice for ING Hubs PH applicants'.*

We obtain your personal data in the following ways:

- You share it with us when you sign an employment contract with us or visit our websites.
- You share it with us directly during your employment at ING Hubs PH.
- From the person who recommended your job application (i.e., through a job referral).
- From your manager or other colleagues, during the course of your employment, such as for performance reviews or peer reviews.
- From other available sources such as professional registers; online or traditional media; publicly available sources (such as Thompson Reuters, World Check, NFIS, or judicial platforms); other ING companies; or third parties such as public authorities or other entities that you provide specific authorization to release your personal data to ING Hubs PH or its legally authorized representatives or agents (e.g. previous employers or personal/professional references), including as part of employee screening.
- We collect audio-visual data, where applicable and legally allowed, for closed-

- circuit television surveillance videos ('CCTV') of ING Hubs PH offices and car parks.
- The administration of the building within which our offices are located may share your personal data with us, as necessary.

## 2. The types of personal data we process.

**Personal data** refers to any information that identifies you or can be linked to a natural person. Personal data we process about you includes:

- **Identification data**, such as your first name, middle name, surname, date and place of birth, ID number, passport number, other data in your ID document, driver's licence, passport or other document confirming your identity, social security number, tax identification number, home address or place of residence, phone number, and email address.
- **Personal information**, such as nationality; gender; work permits; photographs; information about time off work (e.g. sickness, annual leave or other types of leave); professional experience (profile, previous employers, termination of last employments, and work carried out, special projects, outside positions); education, professional qualifications, and continuous training (diplomas, certificates, internships); documents confirming your right to use a vehicle for business purposes or to perform other work-related obligations (e.g. driving licence, registration certificate, insurance policy); work-performance data; access to ING Hubs PH premises; emergency contacts.
- **Financial data**, such as salary information, bank account number, expenses, payslips, credit worthiness, company participations, and transactions.
- **Socio-demographic data**, such as whether you have a spouse, partner, and/or children.
- **Dependent(s)' data**, such as identification data and contact information of your spouse/partner, parent(s), child(ren), or other dependents.
- **Emergency contact person data**, such as identification data and contact information of your emergency contact person(s).
- **Online behaviour and use of ING IT assets**, such as web pages you visit, your IP address, your applications and digital equipment, use of social media and the use of business email.
- **Interests and needs**, for example hobbies and memberships you share with us, career track, skills and behaviour.
- **Audio-visual data**, where applicable and legally allowed, we process CCTV surveillance videos of ING Hubs PH offices and car parks; images, videos, or audio recordings from ING Hubs PH events; images, videos, posts shared by ING Hubs PH employees in media platforms authorized by ING Hubs PH; recordings of phone calls to our service centres or video conversations with customers, employees, and affiliates of ING Hubs PH. Photographs may also be used to provide an access badge to our offices.

## Sensitive data

Sensitive data as defined under the DPA is personal information relating to your (1) race, ethnic origin, marital status, age, color, and religious, philosophical, or political affiliations; (2) health, education, genetic, or sexual life, or to any proceeding for any offense committed or alleged to have been committed by such individual, the disposal of such proceedings, or the sentence of any court in such proceedings; (3) issued by government agencies peculiar to an individual which includes, but is not limited to, social security numbers, previous or current health records, licenses or its denials, suspension or revocation, and tax returns; and (4) specifically established by an executive order or an act of Congress to be kept classified.<sup>1</sup>

We may process your sensitive data if

- you have given your consent, specific to the purpose prior to the processing, or in the case of privileged information, all parties to the exchange have given their consent prior to processing<sup>2</sup>;
- it is legally required and allowed to do so under existing laws and regulations.<sup>3</sup> For example, we may be obliged to keep a copy of your passport or identification card;
- necessary to protect your (or another person's) life and health, and you are not legally or physically able to express consent prior to the processing<sup>4</sup>;
- necessary to achieve the lawful and non-commercial objectives of public organizations and their associations: Provided, That such processing is only confined and related to the bona fide members of these organizations or their associations: Provided, further, That the sensitive personal information are not transferred to third parties: Provided, finally, That consent of the data subject was obtained prior to processing<sup>5</sup>;
- necessary for purposes of medical treatment, is carried out by a medical practitioner or a medical treatment institution, and an adequate level of protection of personal information is ensured<sup>6</sup>;
- necessary for the protection of lawful rights and interests of natural or legal persons in court proceedings, or the establishment, exercise, or defense of legal claims, or when provided to government or public authority<sup>7</sup>.

For example, we process sensitive data related to:

- Administering pensions, healthcare plans, leave programmes or financial aid for

---

<sup>1</sup> Section 3, par. I., Data Privacy Act of 2012 (Republic Act No. 10173).

<sup>2</sup> Section 13(a), Data Privacy Act of 2012 (Republic Act No. 10173).

<sup>3</sup> Section 13(b), Data Privacy Act of 2012 (Republic Act No. 10173).

<sup>4</sup> Section 13(c), Data Privacy Act of 2012 (Republic Act No. 10173).

<sup>5</sup> Section 13(d), Data Privacy Act of 2012 (Republic Act No. 10173).

<sup>6</sup> Section 13(e), Data Privacy Act of 2012 (Republic Act No. 10173).

<sup>7</sup> Section 13(f), Data Privacy Act of 2012 (Republic Act No. 10173).

various health conditions (i.e. processing health data linked to documents that you provide directly to us).

- Providing workplace infrastructure and any additional security requirements when needed.
- Addressing potential special needs, including business continuity and incident/crisis management, to ensure an adequate, safe and secure work environment.
- COVID-19 and health screening protocols. We may run a temperature check when you enter ING Hubs PH office premises and ask you to confirm whether you have been exposed to a person who has tested positive for COVID-19. This is for purposes of securing ING Hubs PH premises and protecting ING Hubs PH employees' health and safety.

### 3. What we do with your personal data.

Processing refers to every activity that can be carried out in connection with personal data, such as collecting, recording, storing, retrieving, consulting, consolidating, adjusting, organising, using, disclosing, transferring, or deleting, blocking, erasing, or destroying it in accordance with applicable laws. Processing may be performed through automated means, or manual processing, if the personal data is contained or is intended to be contained in a filing system.<sup>8</sup>

We only use your personal data for the following business purposes:

#### Human resources and personnel management

As your employer, we process information about you that is necessary to fulfil our contractual obligations (as per your employment or other contract), or to take necessary steps at your request before entering into a contract. We also process information about you when we have a legal obligation to do so, or it is in our legitimate interest, such as for administrative purposes, and to manage our relationship with you. Activities falling under this purpose include recruitment and outplacement, pre-employment, periodic and enhanced employee screening, compensation and benefits, payments, tax issues, career and talent development, insider trading regulations, performance evaluations, training, travel and expenses, employee communications, workforce analytics, international assignments, internal mobility, dispute resolution and litigation.

#### Executing business processes and internal management

To fulfil the employment or training or other contract, our legitimate interest or our legal obligations, we may process information about you for activities such as scheduling work, recording time, managing company assets, providing centralised processing facilities for

---

<sup>8</sup> Section 3, par. o, Implementing Rules and Regulations of the Data Privacy Act of 2012.

greater efficiency to include the use of your data for testing to these facilities conducting internal audits and investigations, implementing insider trading and other similar regulations, implementing business controls, business continuity and incident/crisis management procedures, and facilitating efficient and effective electronic communications within ING Hubs PH. Calls made using identified phone lines are recorded if required for documentation or based on legal requirements.

### **Sharing on social media**

For ING, like most organizations, social media plays a crucial role in connecting people and developing relationships. This is to bolster public knowledge of ING Hubs PH in order to, among others, attract talent for recruitment purposes. ING Hubs PH may share on social media platforms accessible by the public names of ING Hubs PH employees and their roles in ING Hubs PH, images, videos, or audio recordings from ING Hubs PH offices or ING Hubs PH events, whether set up directly or sponsored by ING Hubs PH.

### **Health, safety, and security**

This purpose covers activities related to your wellbeing. To fulfil our legitimate interests, or a public interest, and to comply with our legal obligation as your employer to keep you safe and healthy at work, as well as to protect ING Hubs PH's assets, products, services and reputation, we process data that authenticates your employee status, access rights, monitors your compliance with ING Hubs PH's regulations, or confirms the status of your health. We process your personal data to provide you access to our offices and as part of ensuring that our offices remain secure, our security management team may process your personal data.

### **Organisational analysis and development and management reporting**

This purpose addresses activities such as conducting employee surveys (both locally and globally), managing mergers, acquisitions and divestitures, and processing your personal data for management reporting and analysis, which is performed to fulfil a legitimate interest.

### **Compliance with legal obligations**

In certain instances, we have a legal obligation to process certain personal data to comply with the laws, regulations, and sector-specific guidelines that ING Hubs PH is subject to. For example, to fulfil employee due diligence or sanctions screening requirements under laws and regulations against money laundering, terrorism financing and fraud.

### **Protecting your vital interests**

It may be necessary to process personal information to protect your vital interests, for example in a medical emergency.

### **Preventing and detecting fraud and data security**

We have a legal duty and a legitimate interest to safeguard ING Hubs PH and its affiliates' security and integrity as well as that of the financial sector as a whole. This means collecting information that will help us identify, prevent and investigate activities that could have a negative effect on ING Hubs PH, its affiliates, or other financial institutions; defend, prevent and trace actual or attempted conduct that is criminal or undesirable; use and participate in sector-specific and other warning systems and comply with our legal requirements and regulations against money laundering and terrorist financing. This includes detecting and preventing the loss of personal data, as well as the loss or theft of intellectual or physical business property.

When processing personal data that is not compatible with one of the purposes above, we ask for your explicit consent, which you may withhold or withdraw at any time.

#### **Limitations on processing data of your dependent(s) and/or emergency contact(s)**

ING Hubs PH may process the personal data of your dependent(s) and/or emergency contact(s) if:

- You (and your dependent(s) and emergency contact(s)) have provided the data with consent, and
- it is reasonable and necessary for fulfilling your employment contract or for managing our employment relationship, or
- it is legally required or permitted under local law.

By providing the personal data of your dependent(s) and emergency contact(s), you guarantee that you are specifically authorized by such dependent(s) and emergency contact(s) to provide such information to us.

#### **Retention and deletion of your personal data**

We are legally required to retain your personal data for a specified period of time. This retention period may vary from a few days to years, depending on the applicable local law. When we no longer need your personal data for the process or activity, we originally collected it for, we delete it, or aggregate it (bundle data at a certain abstraction level), render it anonymous and dispose of it in accordance with the applicable laws and regulations.

Unless retention for a longer period is required for legal or reasonable cause, your (and your dependent(s)' and emergency contact(s)') personal data will be deleted, erased, or destroyed upon the lapse of retention period, in accordance with applicable laws, regulations, and applicable internal policies such as, but not limited to, the ING Hubs PH Record Retention Policy. In doing so, we will employ different data destruction methodologies, including but not limited to:

- Permanently deleting the relevant personal data in our data processing systems.



- Destroying any physical copies of personal data that were collected and stored.
- Overwriting personal data that were collected and stored, so that it is beyond use.

To know more about ING Hubs PH's Retention Schedule and Record Retention Policy, you may contact us through the contact details provided in section 9.

#### 4. Who we share your data with and why

We share certain data internally (with other ING businesses/departments) and externally (with third parties outside of ING), if necessary to achieve the purpose(s) in section 3.

Whenever we share personal data in countries outside of the European Economic Area ('EEA') -- whether internally or with third parties -- we ensure there are safeguards in place to protect it. For this purpose, we rely on (among others):

- Binding corporate rules as defined in EC Regulation (EU) 2016/679. These are known as the ING Global Data Protection Policy ('GDPP') and have been approved by the data protection authorities in all EU member states.
- Applicable local laws and regulations, including the Data Privacy Act of 2012.
- [EU Model clauses](#), when applicable. We use standard contractual clauses in agreements with service providers to ensure personal data transferred outside of the EEA complies with EU General Data Protection Regulations ('GDPR').
- Adequacy decisions by the European Commission, which establish whether a country outside of the EEA ensures personal data is adequately protected.

#### ING entities

We transfer data across ING businesses and branches for various purposes (see section 'What we do with your personal data'). We may also transfer data to centralised storage systems or for processing centrally within ING for efficiency purposes. For all internal data transfers, we rely on our GDPP and on the applicable local laws and regulations.

#### Authorised ING Hubs PH employees

Certain employees are authorised to process your personal data for legitimate purposes (see section 3 'What we do with your personal data'). They are only authorised to do so to the extent that is needed for that purpose and to perform their job. All employees are subject to confidentiality obligations, also according to local requirements.

#### Customers or other service centre callers

Calls made using identified phone lines are recorded if required for documentation or based on legal requirements. When a customer expressly requests it, we may disclose the recording or script of a call made to an ING service centre.

### Government, supervisory and judicial authorities

To comply with our regulatory obligations, we may disclose data to the relevant government, supervisory or judicial authorities. In some cases, we are obliged by law to share your data with external parties, including:

- Public authorities, regulators, and supervisory bodies such as the central banks and other financial sector supervisors in the countries where we operate.
- Tax authorities may require us to report your assets (e.g. your salary). We may process your social security number or tax identification number for this.
- Judicial/quasi-judicial/administrative/investigative or other authorities such as the police, public prosecutors, courts and arbitration/mediation bodies on their express and legal request.

Examples of when we may disclose your personal information:

- It is required or permitted by an applicable law or regulation. We endeavor to not disclose more personal information than is specifically required. For example, in case of theft at premises, the police may ask us data about all visitors on a particular day.
- It is requested for a valid legal process such as a search warrant, subpoena or court order.

### Service providers and other third parties

When it is required for a particular task, we may share your personal data with external service providers or other third parties who carry out certain activities for ING Hubs PH in the normal course of our business.

Service providers support us with activities like:

- performing certain services and operations such as background checks for applicants or employee screening as required under internal policies;
- designing, developing, testing, and maintaining internet-based tools and applications;
- IT services such as applications or infrastructure (e.g. cloud services);
- preparing reports, statistics, employee performance assessments, surveys, printing materials and product design, and related Human Resources analyses for internal management and management reporting;
- recruitment and
- payroll services;
- administration of pension fund accounts; and
- securing access to ING Hubs PH offices and assets, and logging of employees, guests, and visitors in its offices.

### Researchers

We are always looking for new insights to help you get ahead in life and in business. For this, we may exchange personal data (when it is legally allowed) with partners like universities and other independent research institutions, who use it in their research and innovation. This personal data is shared at an aggregated level and, as far as possible, the results of the research are anonymous (this cannot be guaranteed e.g. when benchmarking job positions).

### **Those who may follow official ING Hubs PH social media pages**

As mentioned in section 3, for ING, like most organizations, social media plays a crucial role in connecting people and developing relationships. This is to bolster public knowledge of ING Hubs PH in order to, among others, attract talent for recruitment purposes.

In all of these cases, we ensure the third parties can only access personal data that is necessary for their specific tasks or business purpose.

## **5. Your rights and how we respect them**

You have certain privacy rights when it comes to processing of your personal data. These rights may vary from jurisdiction to jurisdiction, depending on the applicable laws. If you have questions about which rights apply to you, please contact us via the contact details in section 9.

We respect the following rights:

### **Right to be informed**

You have to be informed through this Privacy Notice as to when and how your personal data is being processed.

### **Right to access information**

You have the right to ask us for an overview of your personal data that we process and/or a copy of this data.

### **Right to rectification**

If your personal data is incorrect, you have the right to ask us to rectify it. If we have shared data about you with a third party, we will also notify that party of any corrections made.

### **Right to object to processing**

You can object to us using your personal data for our own legitimate interest – if you have a justifiable reason. We will consider your objection and assess whether there is any undue impact on you that would require us to stop processing your personal data.

You may not object to us processing your personal data if

- we are legally required to do so, or
- it is necessary for fulfilling a contract with you.

### **Rights regarding the use of automated decisions**

When it is legally permissible, we sometimes use systems to make automated decisions based on your personal information that are necessary for fulfilling a contract with you. If automated decisions are used, we will inform you about this and the purpose for and the extent of such processing. You have the right to object to such automated decisions and ask for an actual person to make the decision instead.

### **Right to restrict processing**

You have the right to ask us to restrict using your personal data if

- you believe the information is inaccurate;
- we are processing the data unlawfully;
- ING Hubs PH no longer needs the data, but you want us to keep it for use in a legal claim; or
- you have objected to us processing your data for our own legitimate interests.

### **Right to data portability**

You have the right to ask us to transfer your personal data directly to you or to another company. This applies to personal data we process by automated means and with your consent or on the basis of a contract with you. Where technically feasible, and based on applicable local law, we will transfer your personal data.

### **Right to erasure**

We are legally obliged to keep certain personal data for a specified period of time. You may ask us to erase your personal data and the right to be forgotten is applicable if:

- we no longer need your personal data for its original purpose;
- you withdraw your consent for processing it;
- you object to us processing your personal data for our own legitimate interests and we find your claim to be legitimate;
- we unlawfully process your personal data; or
- a local law requires ING Hubs PH to erase your personal data.

### **Right to complain**

Should you not be satisfied with the way we have responded to your concerns, you have the right to submit a complaint to us. If you are unhappy with our reaction to your complaint, you can escalate it to the ING Hubs PH Data Protection Officer ('DPO').

### **Exercising your rights**

If you want to exercise your rights or submit a complaint, please contact us via the contact details under section 9.

If the requirements for your request (as set out in the GDPP for employees, as locally adopted) are not fulfilled, your request may be denied. If permitted by law, we will notify you of the reason for denial.

We aim to address your request within one (1) month of ING Hubs PH receiving the request. Should we require more time to complete your request, we will let you know how much longer we need and provide reasons for the delay.

If you have reasonable and legitimate basis to believe that your or your dependent(s)' or emergency contact person(s)' personal data has been misused, maliciously disclosed, or improperly disposed, or if any of the rights discussed here have been violated, you have the right to submit a complaint to the ING Hubs PH DPO and thereafter, to the Bank DPO.

If, upon exhausting all internal remedies available within ING Hubs PH, your concerns are still not addressed, you may escalate it to the local data protection authority (National Privacy Commission ('NPC')).<sup>9</sup>

The contact information of the ING Hubs PH DPO, the Bank DPO, and the NPC are found in section 9.

You may refer to the ING Hubs PH Policy on the exercise of individual rights at the ING Hubs PH Policy House on SharePoint for the specific procedure and forms to be used.

## **6. Your duty to provide data.**

As your employer, there are specific personal information that we are legally required to collect, or that we need in order to execute our duties and fulfil our contractual obligations. There is also information that we need for certain human resources processes, or for us to adequately secure our premises and, when necessary, during an emergency, to assist you. We aim to only ask you for personal data that is strictly necessary for the relevant purpose. Not providing this information may mean that we cannot maintain your contract or provide certain benefits to you and/or your dependent(s).

---

<sup>9</sup> Local administrative agencies follow the rule of exhaustion of remedies. Under NPC Circular No. 16-04 (Rules of Procedure), the NPC would require the complainant to show that ING Hubs PH had a chance to address the issue before escalating the matter to the NPC.

## 7. How we protect your personal data

We take appropriate physical, technical, and organisational measures (policies and procedures, IT security etc.) to ensure the confidentiality and integrity of your personal data and the way it is processed. We apply an internal framework of policies and minimum standards across all our business to keep your personal data safe. These policies and standards are periodically updated to remain current with regulations and market developments.

In addition, ING Hubs PH employees are subject to confidentiality obligations and may not disclose your personal data unlawfully or unnecessarily. To help us continue to protect your personal data, you should always contact ING Hubs PH if you suspect your personal data may have been compromised.

## 8. Changes to this Privacy Notice.

We may amend this Privacy Notice to remain compliant with any changes in law and/or to reflect how we process personal data. This document was updated in November 2024.

## 9. Contact and questions.

To find out more about ING Hubs PH's data privacy policy(ies) and how we use your personal data, please see the ING Hubs PH Policy House on SharePoint. You can also find contact information below.

ING Hubs PH <b>Data Protection Executive Office</b>	ING Hubs B.V. Philippine Branch 27/F World Plaza Building, 5th Avenue, E- Square Zone, Crescent Park West, Bonifacio Global City, Taguig, Philippines Email: <a href="mailto:INGHubsPH.DPE@ing.com">INGHubsPH.DPE@ing.com</a>
ING Hubs PH <b>Data Protection Officer</b>	ING Hubs B.V. Philippine Branch 27/F World Plaza Building, 5th Avenue, E- Square Zone, Crescent Park West, Bonifacio Global City, Taguig, Philippines Email: <a href="mailto:INGHubsPH.DPO@ing.com">INGHubsPH.DPO@ing.com</a>
Bank Data Protection Officer Office	<a href="mailto:dpo.office@ing.nl">dpo.office@ing.nl</a>
National Privacy Commission (Philippines data protection authority)	<a href="https://privacy.gov.ph/">https://privacy.gov.ph/</a>

## 10. ING Hubs PH – Seal of Registration issued by the National Privacy Commission



## EMPLOYEE PRIVACY CONSENT FORM

I hereby consent to the processing of my personal data by ING Hubs B.V. Philippine Branch ('ING Hubs PH') for the purpose(s) provided in the Privacy Notice for ING Hubs PH employees ('Privacy Notice'), the terms of which are incorporated herein by reference.

This consent covers my Personal Data and Sensitive Personal Data, as well as the Personal Data of relevant individuals whose information was provided by me, my authorized representatives or third parties. I am aware of my rights and how to exercise them, as provided under the Privacy Notice.

**By affixing my name and signature below, or by clicking on the tick box that is linked to this document, I affirm that I have read, understood, and agree to the terms outlined in the Privacy Notice and this Consent Form.**

Joselito Buenaventura

EMPLOYEE NAME



EMPLOYEE SIGNATURE

September 1, 2025

DATE SIGNED