



**Information Security and
Data Protection**

We are world leaders in digital HR solutions

We are committed to helping our clients select and manage the best talent. That is why we created Pandapé, the most popular suite of HR solutions in Latin America.

We designed Pandapé to help you to streamline, transform, and improve your recruitment processes. With this solution you will innovate your HR management, improves communication and increases performance.

At the heart of our success is our focus on information security and data protection.



Table of Contents

Information Security

<u>ISO 27001 Certification</u>	4
<u>Cloud Computing</u>	5
<u>Operations Security</u>	6
<u>Secure Development</u>	7
<u>Availability and Continuity</u>	8
<u>Vulnerabilities Management</u>	9
<u>Services Security</u>	10

Data Protection

<u>Our pledge</u>	12
<u>Processor</u>	13
<u>Principles</u>	14
<u>Privacy by design and default</u>	15
<u>Processing</u>	16
<u>Purposes</u>	17
<u>Rights</u>	19
<u>Retention</u>	20
<u>Transfers</u>	21
<u>Subprocessors</u>	22
<u>Security</u>	23
<u>Breaches</u>	24



We are committed to information security in our services

We have an Information Security Management System (ISMS) certified under the **ISO/IEC 27001:2022** standard for the services that we offer. This includes **Pandapé**.

Our processes and systems are subject to regular audits, penetration testing, intrusion detection and prevention. We monitor and improve our technology, infrastructure and processes to ensure maximum quality, efficiency and security.

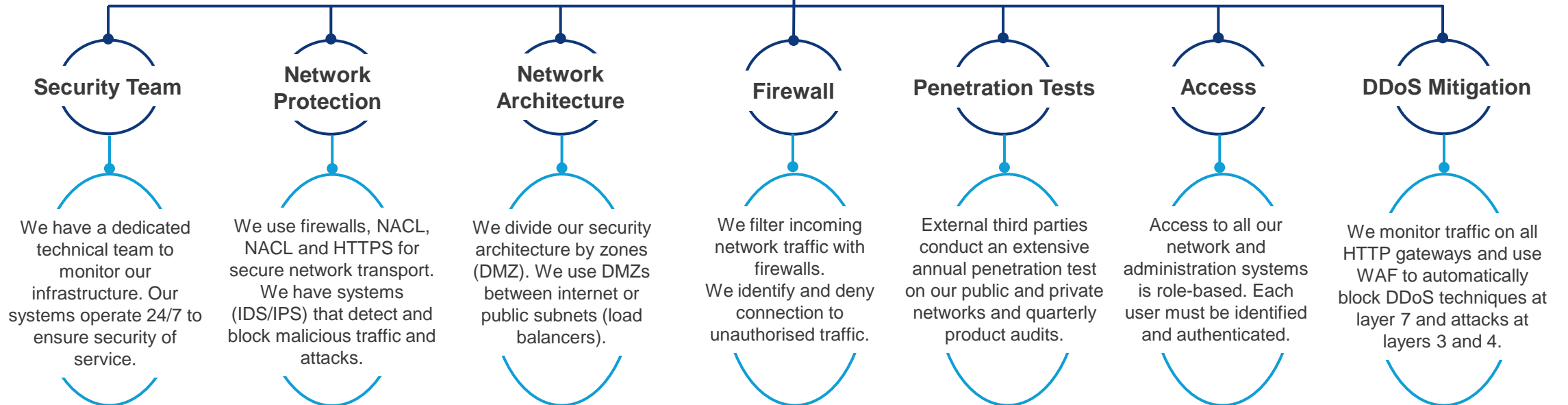




Cloud Computing

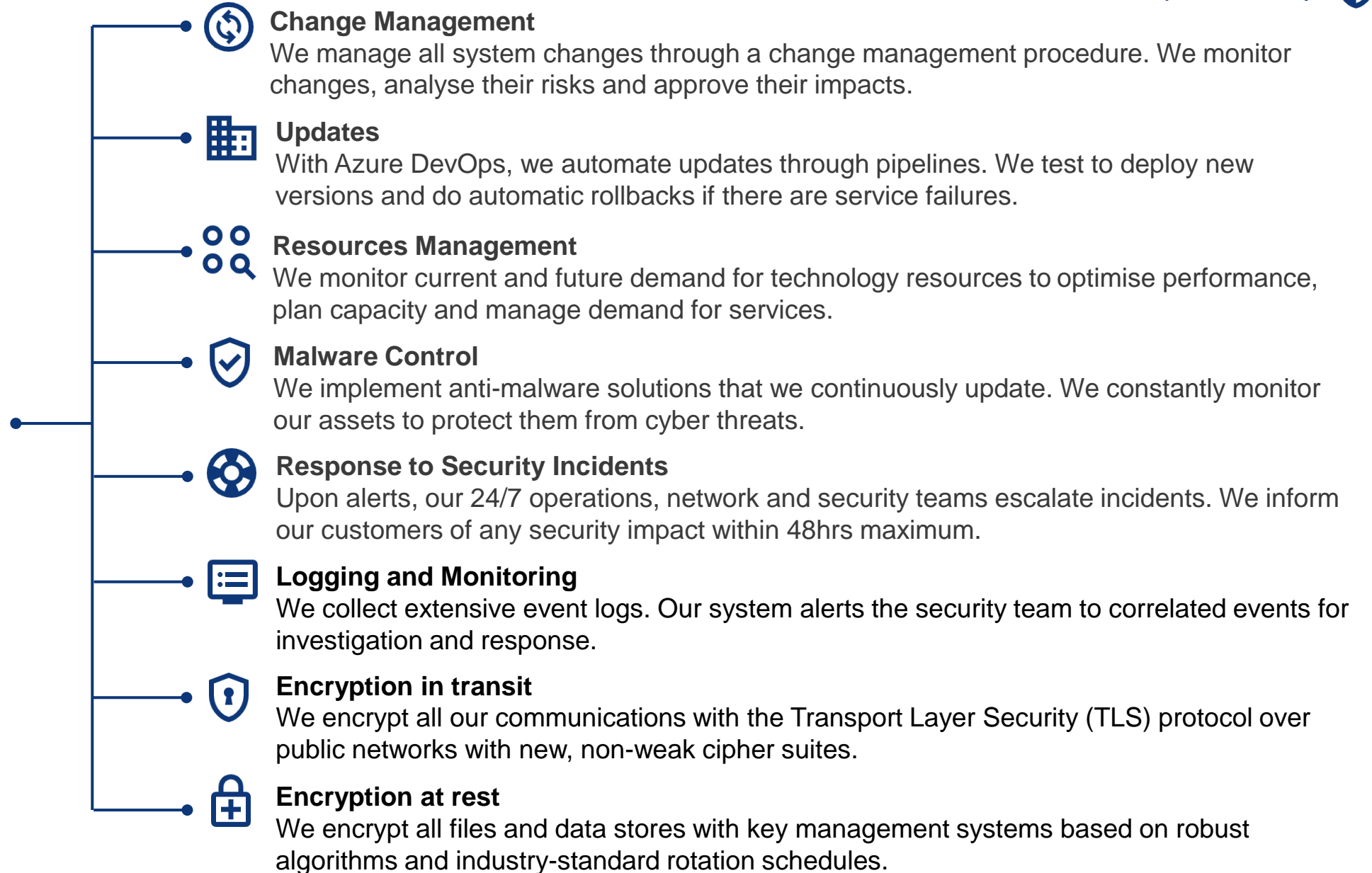
AWS and Azure are our cloud computing providers.

We draw on the expertise, resources and reputation of Amazon and Microsoft to ensure secure, robust and reliable cloud operations.





Operations Security





Secure Development

As part of our Secure Development Life Cycle (SDLC), we have several tools that we use at every stage of software development to ensure the security of our services from conception to implementation and maintenance.



Language

Our software stack is based on various programming languages for our websites and APIs. Azure DevOps supports programming languages with high scalability, reliability and security.



Security Training

We train our developers internally on code security, design, following best practices to combat common attacks and using security controls.



Quality Assurance

Our QA team reviews and tests our code, integrating various manual and automated tests so that only code that has been evaluated and approved is implemented.



Audit Logs

We keep records of all accesses and changes made by each user (audit logs). Logs are stored under restricted access and can only be consulted in the event of an incident.



OWASP Security Checks

We align our software development with OWASP industry practices. These include controls that reduce our exposure to Cross-Site Scripting (XSS), Cross-Site Request Forgery (CSRF) and SQL Injection (SQLi), among others.



Isolated Environments

We physically and logically separate test, staging and development environments. We do this separation through network isolation, firewalls and NACL. We do not use real production data in the development or test environments.



Availability and Continuity



Redundancy

Our production services infrastructure has redundancy to avoid single points of failure. If a primary system fails, redundant hardware relieves it. We use service bundling and network redundancy to reduce single points of failure.



Backup

AWS/Azure provide our backup infrastructure that resides in long-term data stores behind logically secured and encrypted private networks at rest. We back up data from production environments daily and weekly, through a random check, we verify the integrity of the backup.



Disaster Recovery

Our plan ensures availability and disaster recovery of services, through a robust technical environment and recovery plans with vendor redundancy, according to the RTOs and RPOs we define.



Vulnerabilities Management

We have a number of tools that allow us to detect technical vulnerabilities



Internal Dynamic Vulnerability Scanning

We employ qualified third-party security tools to continuously and dynamically scan our applications against OWASP rules, among others. All HTTP controllers have an active WAF that blocks all known OWASP and major known rules in real time.



External Dynamic Vulnerability Scanning

We use industry-standard, customised scanning technologies to efficiently test infrastructure and software while minimising the potential risks associated with active scanning. We perform testing and on-demand scans as needed. Scans are performed during non-peak windows.



Static Code Analysis

Our source code repositories are continuously scanned at test and review stages in CI/CD Pipelines and Flow (continuous integration) and are integrated with all QA flows.



Security Penetration Testing

We rely on external third-party security experts to perform detailed penetration testing and dynamic code analysis.



Security Features in Our Services

These features allow us to preserve the security of the information that circulates or is stored through the use of our services.

Feature	Description
Options for authentication	For Web GUI applications, we offer account login with 2FA. For product APIs and/or customer integrations, we offer an authentication flow with API keys and/or secret/tokens to authenticate and authorise all API calls and actions with the backend. Users accessing the tool are uniquely and uniquely identified through the mandatory authentication system, consisting of a unique user and a password. The system automatically generates an initial key or password that must be changed on 2-factor authentication (2FA) is required for all users. 2FA authentication provides another layer of security to your account, making it difficult for someone else to log in as you. For security reasons, the key or password will be required to contain a specific format to avoid weak keys.
Two-factor authentication (2FA)	2-factor authentication (2FA) is required for all users. 2FA authentication provides another layer of security to your account, making it difficult for someone else to log in as you.
Password policy	Passwords can only be reset by the end user with an email address. The end user can generate a temporary password reset URL on the login page. Password policies follow the main recommendations to ensure your security.
Secure credential storage	We follow best practices for secure storage of credentials. All passwords are stored encrypted, i.e. they are never stored in human-readable form. A secure one-way hash is used, with encryption at rest and of all operations in transit to the backend.



Security Features in Our Services (cont.)

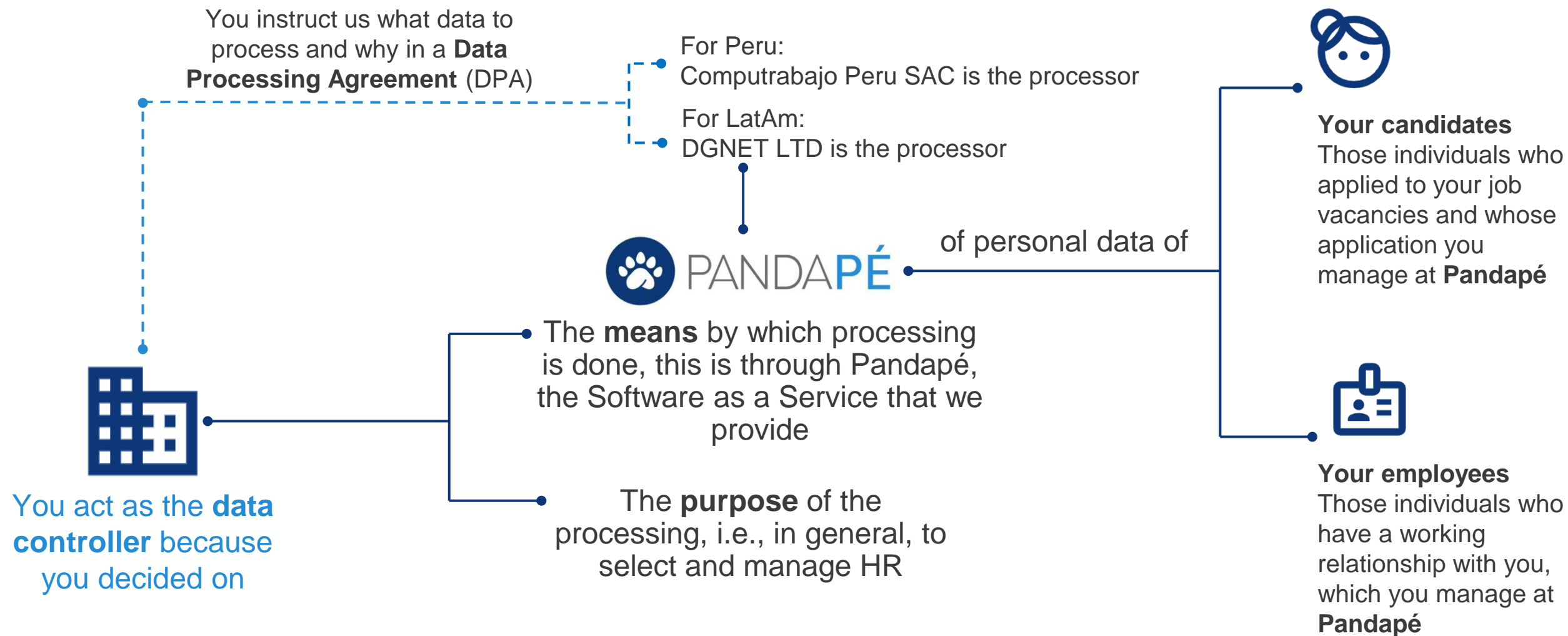
These features allow us to preserve the security of the information that circulates or is stored through the use of our services.

Feature	Description
Access privileges and roles	Access to data is governed by access rights and can be configured to define granular access privileges. Applications have various levels of permissions for users (owner, administrator, agent, end-user, etc.) and a granularity of roles per group.
High availability and accessibility of the product	To ensure low latency and high availability in content delivery, a content delivery network (CDN) is used, which ensures low latency and high availability.
Customer data	Each customer's data and documentation is stored in encrypted form in its own independent logical space.
Private attachments	By default, all instances of our applications are protected, all assets and attachments are private and require a login and permission/role. In addition, all assets and attachments are stored in an encrypted data store.

Our priority is to support you in protecting the personal data of your candidates

At Pandapé, we understand your obligations as the data controller of your candidates' and collaborators' personal data. Therefore, we offer solutions that help you fulfill your responsibilities and respect privacy.

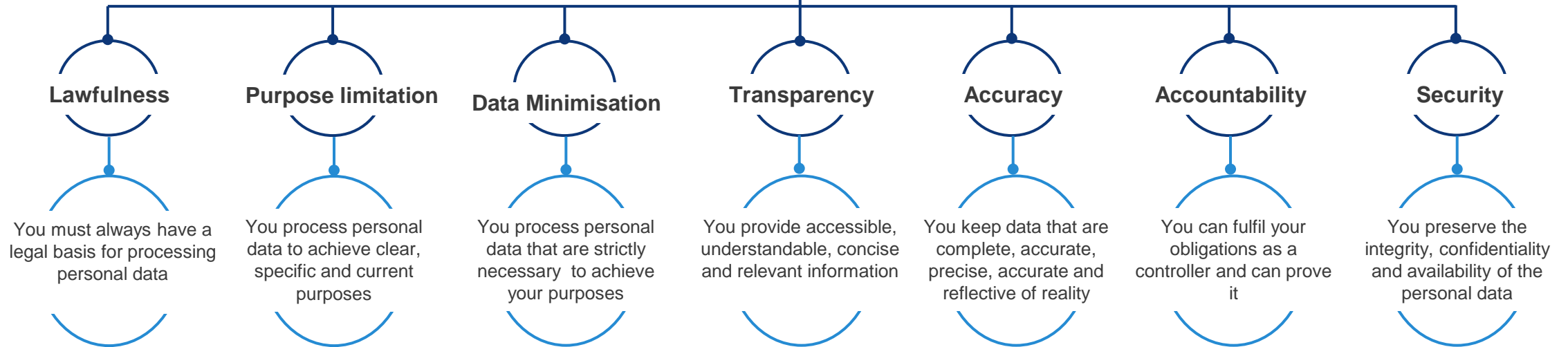
Since our beginning, we have focused on developing solutions focused on personal data protection. This means that, in practice, we develop tools, implement measures, and provide information so that people can make informed decisions and always have control over their personal data.





Principles

As processors, we expect to build a relationship with you (controller) based upon these principles





Pandapé is *privacy-friendly*

We have designed and developed **Pandapé** so that you, as the controller, can give your candidates and employees control of their personal data and let them know what happens to such data. We do not tolerate invasive, misleading or confusing practices that affect privacy.



Privacy by Design

At each stage of development, we have made decisions to:

- Guarantee the confidentiality, integrity, availability and permanent resilience of systems and services
- Restore availability and access in the event of security incidents
- Continuously verify, evaluate and assess the effectiveness of our technical and organisational measures

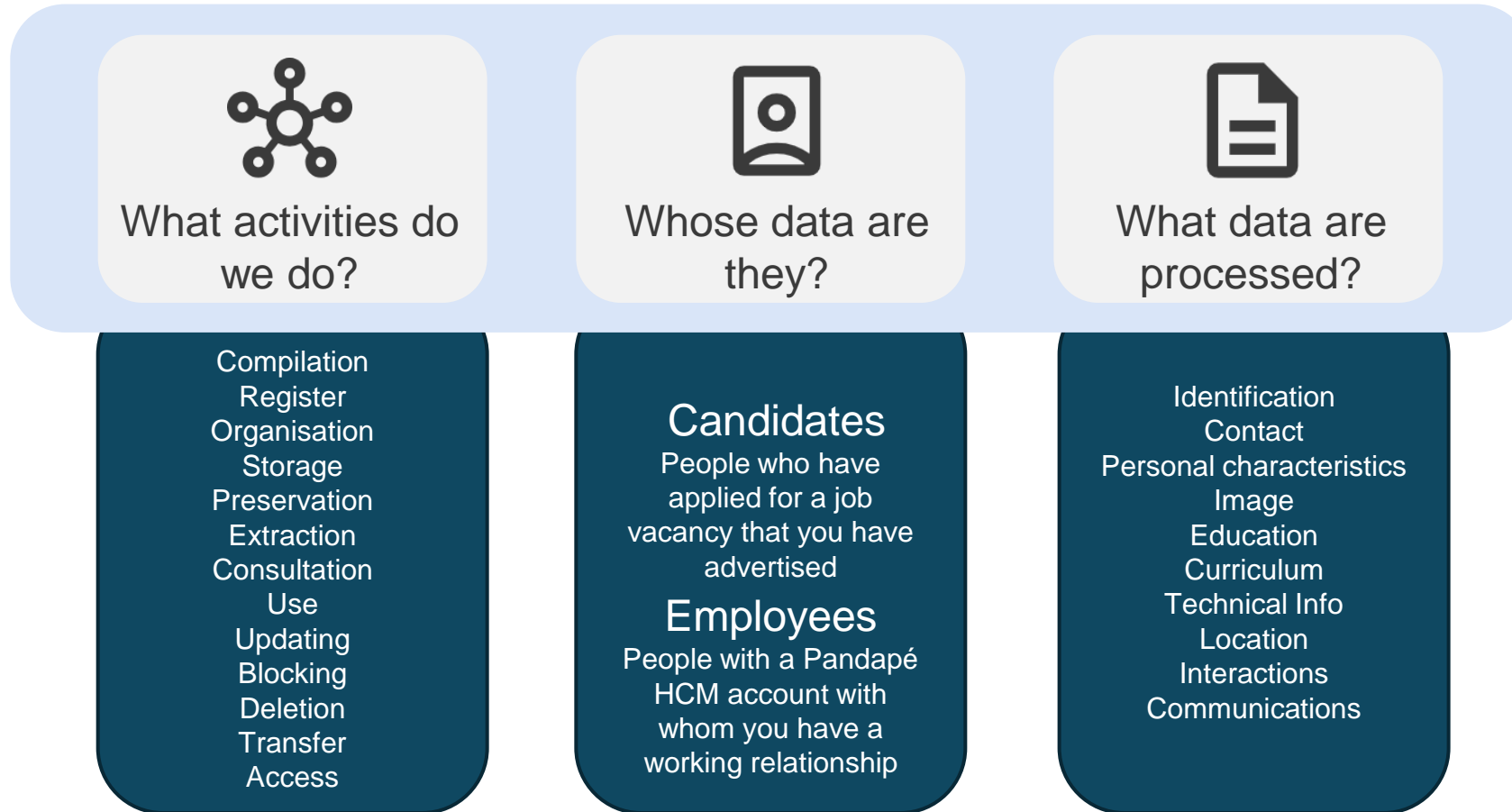


Privacy by Default

Pandapé's original account setup is privacy-friendly, for example:

- There are configurable timers for permanent deletion of personal data
- We offer a privacy policy template for your candidates and/or collaborators
- Various messaging systems and alerts allow your recipients to unsubscribe

Processing of data we do on your instructions





Purposes



As the **data controller**, you are the one **who determines how and for what purpose you will process personal data**. So, it is your duty to answer, *‘why do I want Pandapé?’* and *‘what will I do with my candidates’ and employees’ personal data?’*



We, as **data processors**, cannot tell you what are the purposes or means of data processing. But, by the nature of our solutions, we believe that:

✓ Pandapé ATS will help you to:

- Manage the selection process of your candidates
- Communicate with the candidate to discuss selection processes
- Search for suitable candidates to fill the vacancies you have available

✓ Pandapé HCM will help you to :

- Managing the working relationship with your employees
- Communicate with your employees on work-related issues
- Follow up on your employees’ performance



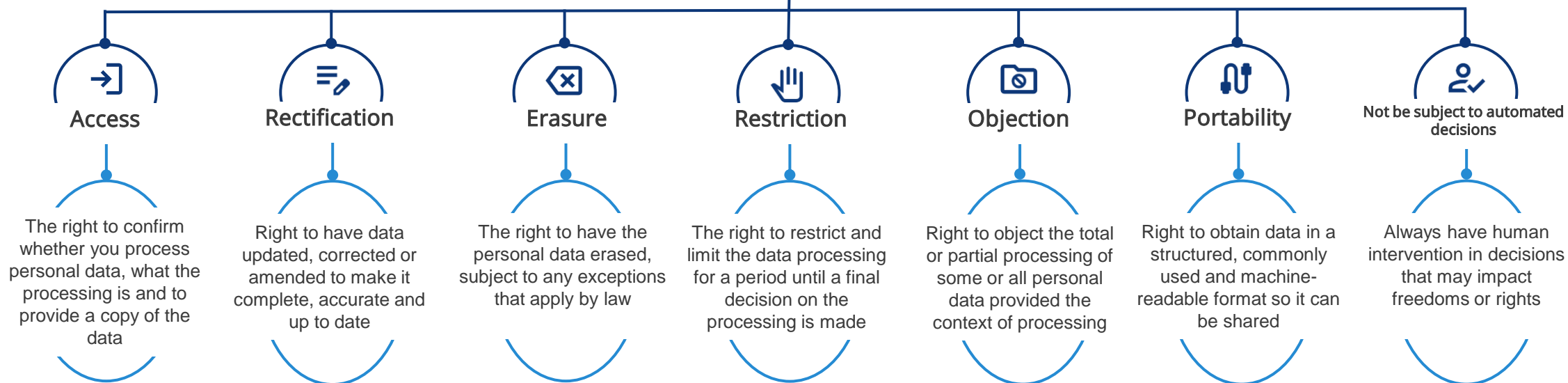
In **Pandapé's** design we include a privacy settings menu where you can autonomously manage retention times, updates to your privacy policy and more.

Thanks to this, your candidates and employees can have updated and complete information about the personal data processing you conduct and information on how to exercise their rights.



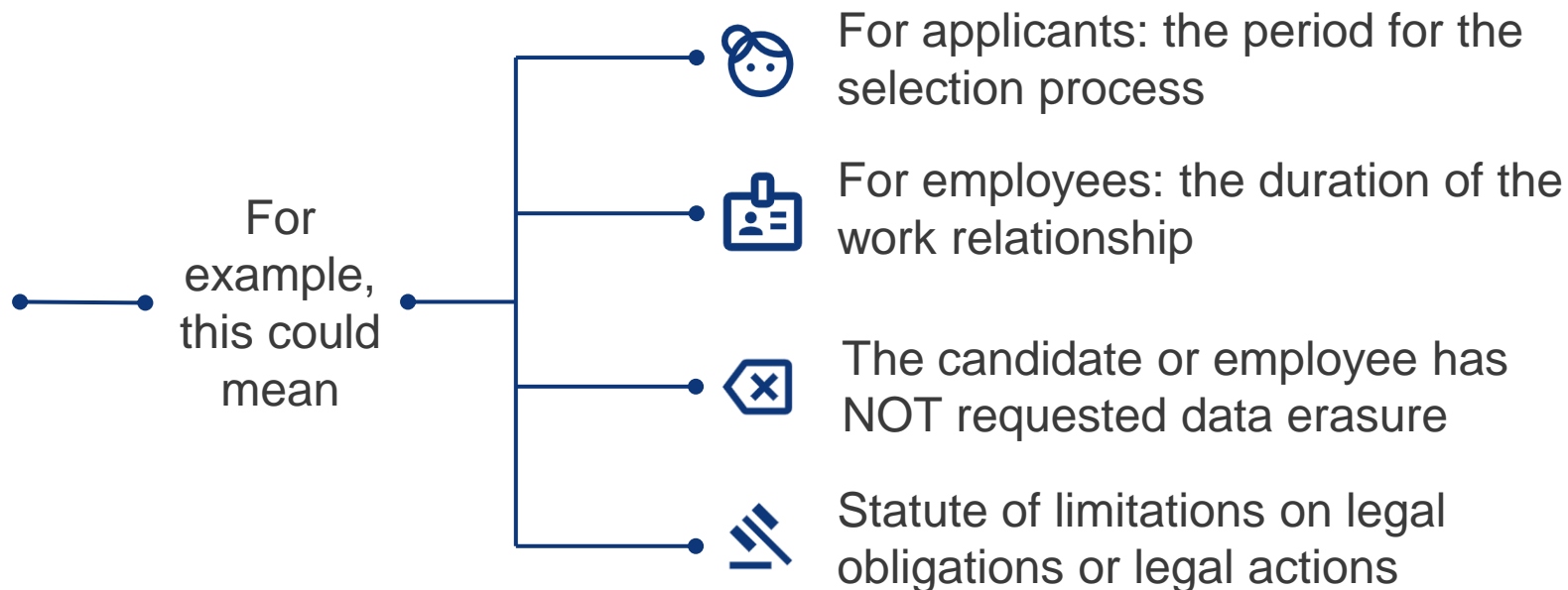
Rights

As a data processors, we can help you, as the data controller, to respond in to requests related to the rights of





As the data controller, you decide how long to keep personal data



The admin users that you assign in **Pandapé** will be able to delete from the system the data for which the retention period has expired



We share data only when it is necessary to fulfil the purposes you specified

These are the third parties with whom we share personal data. Sometimes these third parties are in countries other than that of your candidates or employees.

We make our best efforts to have suppliers that are in countries declared adequate by data protection authorities. In the absence of such a declaration, we implement standard contractual clauses or other mechanisms to maintain the same level of protection as the data has from its place of origin.



Sub-processors

These are third parties or companies within our group of companies that, under our instructions, carry out processing activities. For example: cloud, support, analytics.



Official authorities

They are public entities that in the exercise of their legal and/or regulatory functions may order us to share personal data of their users. In these cases, we will work with you to respond.



About the sub-processors

To provide the **Pandapé** service, we subcontract with third parties who support us in processing personal data on your behalf. Without them, we cannot provide the service. These third parties are **sub-processors for the processing of personal data**. These are the measures we have in place in respect of them:



Due Diligence

At a minimum, our legal, security and data protection experts review:

- Cybersecurity policies, processes and procedures
- Technical and organisational data protection measures
- Service and support agreements



Reputation

We focus on suppliers that:

- Have international cybersecurity or quality certifications
- Have no fines or investigations for security incidents within the past 5 years
- Publish internal and/or external audit reports
- Are reputable and globally known
- Located in a adequate country



Contract

We draft Data Processing Agreements (DPA) that have as a minimum:

- Obligation to follow instructions from the controller
- Audits
- Communication of incidents
- Support for resolving requests to exercise rights
- Protection for international data transfers
- Authorisation for sub-processors



Follow up

After executing the DPA, we monitor the relationship with the manager to:

- Update changes in the business relationship
- Include new legal obligations in the contract
- Monitor data retention policies
- Recognise amendments in sub-processors



Security Measures

These are the practices and tools we implement to ensure the confidentiality, integrity and availability of your candidates' and employees' personal data.

Organisational Measures

- We follow our data protection procedures for development
- We have a Data Protection Officer
- We carry out Data Protection Impact Assessments for high-risk processing
- We train our employees
- We have an information security policy
- We maintain a register of processing activities
- We focus on collecting and processing only the minimum necessary data
- We follow applicable incident management regulations


Technical Measures

- We encrypt data in transit (TLS 1.2) and at rest (AES 256)
- We control access to the portal through user authentication
- We have firewalls, intrusion detection/prevention systems (IDS/IPS)
- We update our antivirus
- Implement DLP technologies
- We store personal data in AWS (ISO 27001)
- We implement automatic monitoring systems to detect and respond to suspicious activity
- We implement separate, pseudonymisation, masking or other techniques as required

Data Breach Management

We take the security of the personal data of our candidates and business users very seriously. We never skimp on protection, but we know the risk is never zero. Something can happen. But when it does, this is what we do:





**Thank you for trusting
Pandapé. The leading
HR management suite in
Latin America.**

**If you have any
questions, please
contact your assigned
executive.**

