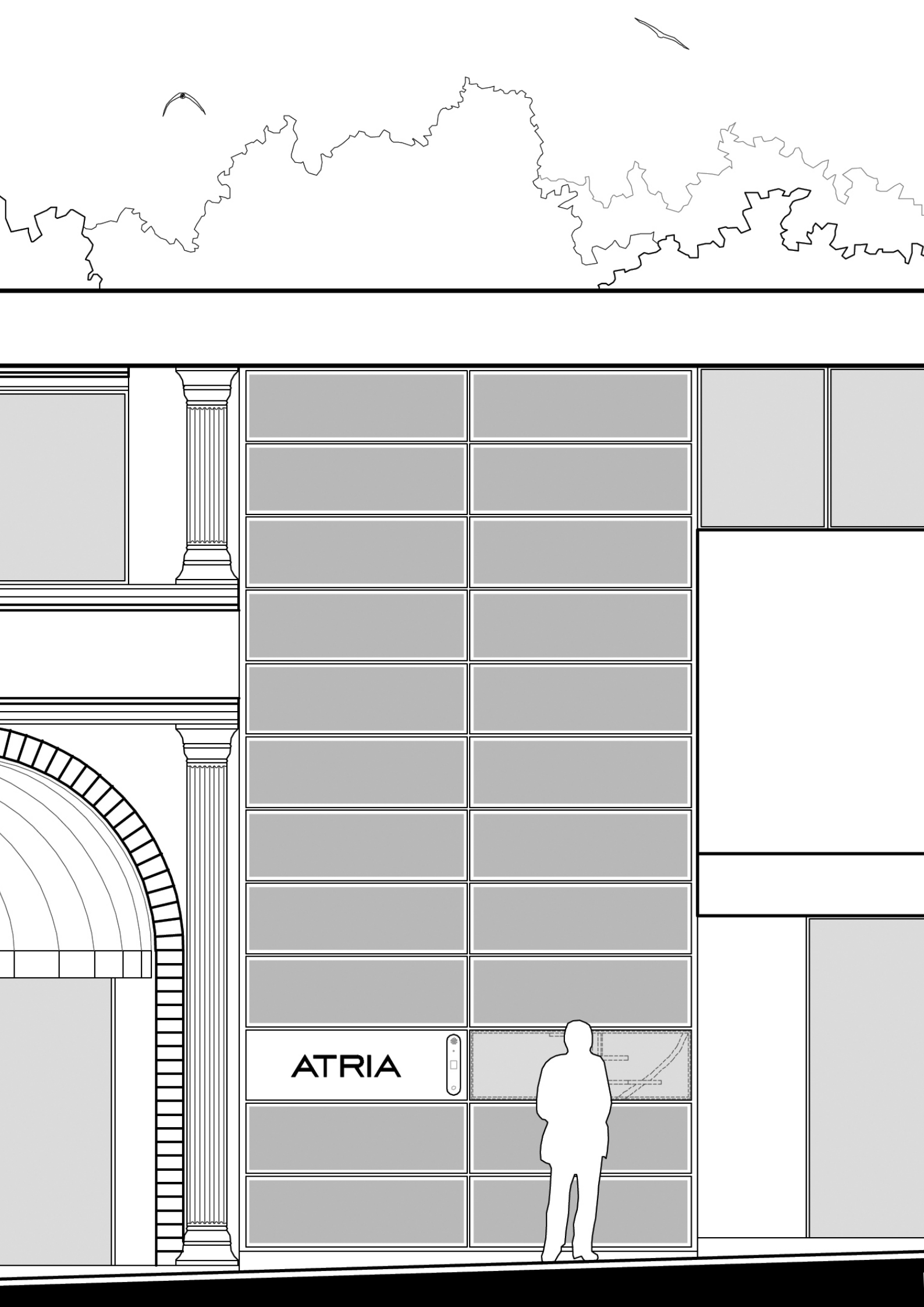
Access to Information Policy

Principles of data managment and confidentiality

ATRIA


ATRIA

Dear Stakeholder:

Atria's Policy on Access to Information has enabled our company to become a reference leader in transparency and has made a consistant change in how our people make information available to the public.

Our principles are based on ethics and transparency with the public and, at the same time, help preserve personal privacy and manage sensible and confidential information with the required accuracy.

We attach great importance to the protection of our stakeholders personal data. We therefore strictly adhere to the legal provisions governing the admissibility of the handling of personal data and have taken appropriate technical and organisational precautions.

The AI Policy also outlines a clear process for making information publicly available and provides important guidelines on how to manage our project's data properly and unreasonably.

The following declaration gives you an overview of how we guarantee this protection and what kind of data we collect, for what purpose.

Kind regards,

Gustavo Costa
Founding Principal

Transparency

We are committed to relate with our internal and external public, lawfully, ethically and with transparency. We believe that data and information shall be used in a way that is adequate, relevant and limited to only what is necessary.

Founded in 2002 by architect Gustavo Costa, Atria is recognized for its activity in architecture, urban planning, engineering, construction management, design and strategic thinking. At the core of our work there is a profound commitment to strive for innovative design solutions, consistent to artistic thinking, aligned with the concepts of environmental preservation and based on a production methodology that is multidisciplinary. We believe working in this manner enables ambitious project solutions, while still allowing us to offer the necessary skills and tools to guarantee our clients the best cost-benefit scenarios.

We are all caretakers of Atria's reputation. How we conduct our business and how we treat others—our fellow partners, customers, communities, suppliers and shareholders—will continue to determine how the world views Atria.

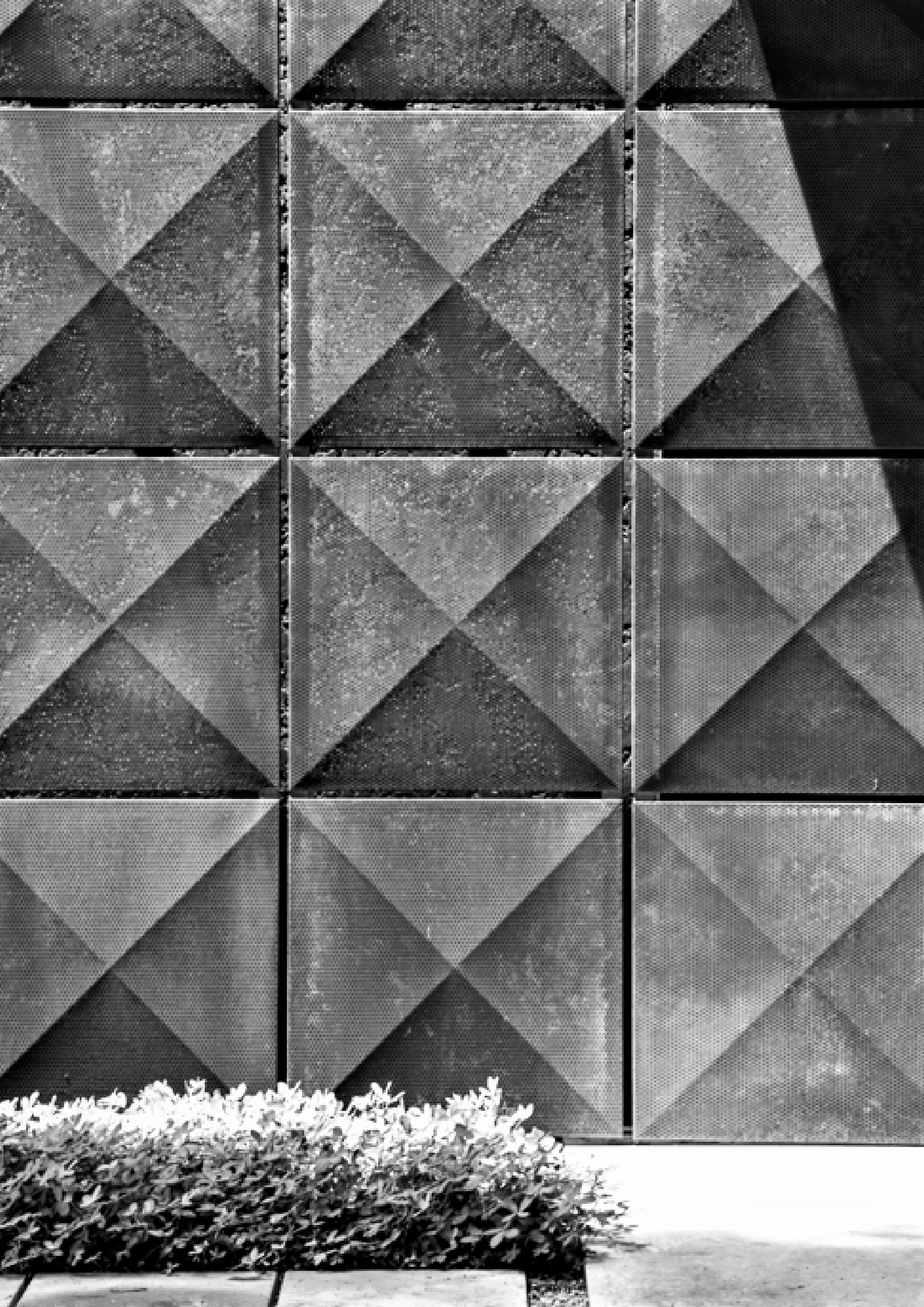
Use data fairly.

Use for specified, explicit purposes.

Limit to the necessary.

Comply with the Policies.

Be accurate.



Content

Privacy principles

General rules

Data Privacy Principles

Our general principles with respect to the collection and processing of personal data and project information is: transparency, legitimate purpose and proportionality.

Transparency

The principle of transparency requires that the purpose for processing a person's data should be determined and disclosed before its collection or as soon as practicable. Also, consent of the data subject on the collection and processing of his data should first be obtained, subject to exemptions provided by laws and regulations. In obtaining his consent, the data subject must be informed of the nature, purpose, and extent of the processing of such personal data, including the risks and safeguards involved, the identity of the personal information controller, his rights as a data subject as well as how these can be exercised. Moreover, information provided to a data subject must always be in clear and plain language to ensure that they are easy to understand and access.

Legitimate Purpose

The principle of legitimate purpose requires that the collection and processing of information must also be compatible with a declared and specified purpose, which must not be contrary to law, morals, or public policy. In other words, personal data and project information should be processed fairly and lawfully.

Principle of Proportionality

The processing of personal data and project information shall be relevant to, and must not exceed, the declared purpose. Any collected information may be retained only for as long as necessary for the fulfillment of the purposes for which the data was obtained or for the establishment, exercise, or defense of legal claims, or as provided by law.

"We handle information in a way that ensures appropriate security."

Privacy principles

What is Expected of Everyone

Everyone responsible for using personal data has to follow strict rules called 'data protection principles'. They must make sure the information is:

- used fairly, lawfully and transparently;

- used for specified, explicit purposes;

- used in a way that is adequate, relevant and limited to only what is necessary accurate and, where necessary, kept up to date kept for no longer than is necessary;

- handled in a way that ensures appropriate security, including protection against unlawful or unauthorised processing, access, loss, destruction or damage.

"We work with clear principles relating to the processing and handling of private data and information."

Intellectual Property and Proprietary Information

Confidential Information

During the course of employment at Atria, all partners gain some knowledge and information that is non-public and belongs to Atria or its Clients and Stakeholders. Partners are trusted with maintaining the confidentiality of this valuable information.

Confidential information includes things such as supplier information, Atria technologies, projects, documents, business and marketing plans, internal company communications, and existing and future product information. Atria information should be used only for company purposes and should not be disclosed to anyone outside of Atria. Even within the company, only those individuals who truly need to know the information to conduct their business should have access to confidential information. If you leave Atria, you must return all company materials and property, and any copies.

Confidential materials should:

- Be stored in a secure place and should not be left out where others can see them
- Be clearly marked as confidential
- Not be sent to unattended fax machines or printers
- Not be discussed where others may hear

A sample of our "Security Information Compliance Term" is avaiable for referenc on appendix 1 of this Policy.

Due Dilligence

Pre qualification program for sub sonsultants and vendors

Atria established a due diligence system to support its ongoing commitment to meet all of its legal and compliance obligations. Among other purposes, this program is designed based on Brazilian "Empresa Pró Ética" for the "CGU - Controladoria Geral da União", and the Foreign Corrupt Practices Act, as well as the United Kingdom Anti-Bribery Act.

Atria requires that subcontractors and vendors be prequalified to be eligible to work with our company. We seek quality partners in our subcontractors and vendors that share with us the desire to exceed our clients' expectations.

We select subcontractors that are financially healthy, have the necessary resources to complete the project and have a proven track record.

A sample of our "Non-disclosure Agreement" is avaiable for referenc on appendix 1 of this Policy.


34
ATRIA
ATRIA ARQUITETOS – GLS 508 BLOCO C LOJA 34 – (61)

Confidentiality

General Obligations of Staff Members

The sensitive and confidential nature of much of our work requires of staff a high degree of integrity and concern for the interests of the organizations, clients and stakeholders we work with. In addition, as dealing with international organizations and governments, our staff members have a special responsibility to avoid situations and activities that might reflect adversely, compromise operations, or lead to real or apparent conflicts of interest. Therefore, Atria staff members shall:

- discharge their duties solely with the interest and objectives of the stakeholders in view and in so doing shall be subject to the authority of the responsible to him;

- respect the international character of their actitivies and maintain their independence by not accepting any instructions relating to the performance of their duties from any governments, or other entities or persons external to the project Atria is managing. unless on secondment Atria members shall not accept in connection with their appointment or service with the stakeholders any remuneration, nor any benefit, favor or gift of significant value;

- conduct themselves at all times in a manner befitting their status as employees of a company that deal with international organizations. They shall not engage in any activity that is incompatible with the proper discharge of their duties wit. They shall avoid any action and, in particular, any public pronouncement or personal gainful activity that would adversely or unfavorably reflect on their status or on the integrity, independence and impartiality that are required by that status;

- observe the utmost discretion in regard to all matters relating to the stakeholders both while they are staff members and after their service with the Atria has ended. In particular they shall refrain from the improper disclosure, whether direct or indirect, of information related to our projects.

All rights in any work produced by staff members as part of their official duties shall belong to Atria.

Condifentiality

Human Resources

Entering Employment

Atria's recruitment policy seek to attract staff members of the highest caliber appropriate to job requirements under employment terms and conditions that are responsive both to our stakeholders' needs and the staff member's well-being. To that end, Atria is attentive to give paramount importance to securing the highest standards of efficiency and technical competence in appointing staff members and, within that parameter, pay due regard to the importance of recruiting staff on as wide a multi-cultural basis as possible;

Organization and Personal Managment

After someone is recruited and starts working at Atria, the efficient administration of data and information requires that our staff work be conducted within certain generally applicable standards and conditions. At the same time, it is recognized that the changing demands on Atria require that staff also adapt to meet evolving needs and circumstances. To enable Atria to respond effectively in such circumstances, and make sure our staff members are updated with our latest policies, we:

- organize, assign and transfer staff to meet Atria's needs for security, confidentiality and transparency when dealing with our stakeholders'informations and data;

- establish procedures for the periodic review of staff members' work performance in order to promote the most effective use of their expertise, to determine the quality of their service, to recognize their achievements, and to guaranty that their personal data is also being protected;

- establish programs and arrangements for staff training and development for the purpose of updating and improving staff skills to meet the needs of our stakeholders' data security needs;

- establish the best conditions and limits under which staff members may be required to travel, allowing them to comply with the AI Policy also during external missions.

Data Managment

Managing data confidentiality

Our data confidentiality principles are about protecting data against unintentional, unlawful, or unauthorized access, disclosure, or theft.

Atria is specially attentive to privacy of information, including authorizations to view, share, and use it. Information with low confidentiality concerns may be considered "public" or otherwise not threatening if exposed beyond its intended audience. Information with high confidentiality concerns is considered secret and must be kept confidential to prevent identity theft, compromise of accounts and systems, legal or reputational damage, and other severe consequences.

Consider the following when managing data confidentiality:

- To whom data can be disclosed;
- Whether laws, regulations, or contracts require data to remain confidential;
- Whether data may only be used or released under certain conditions;
- Whether data is sensitive by nature and would have a negative impact if disclosed;
- Whether data would be valuable to those who aren't permitted to have it.

Guidelines

Encrypt sensitive files

Encryption is a process that renders data unreadable to anyone except those who have the appropriate password or key. By encrypting sensitive files (by using file passwords, for example), you can protect them from being read or used by those who are not entitled to do either.

Manage data access

Controlling confidentiality is, in large part, about controlling who has access to data. Ensuring that access is only authorized and granted to those who have a "need to know" goes a long way in limiting unnecessary exposure. Users should also authenticate their access with strong passwords and, where practical, two-factor authentication. Periodically review access lists and promptly revoke access when it is no longer necessary.

Physically secure devices and paper documents

Controlling access to data includes controlling access of all kinds, both digital and physical. Protect devices and paper documents from misuse or theft by storing them in safe areas. Never leave devices or sensitive documents unattented in public locations.

"Ensure that access is only authorized and granted to those who have a need to know."

Data Managment

Securely dispose of data, devices, and paper records

When data is no longer necessary, it must be disposed of appropriately. Sensitive and confidential data, must be securely erased to ensure that it cannot be recovered and misused. Devices that were used to store sensitive information should be destroyed or securely erased to ensure that their previous contents cannot be recovered and misused.
Paper documents containing sensitive information should be shredded rather than dumped into trash or recycling bins.

Manage data acquisition and utilization

When collecting sensitive data, be conscious of how much data is actually needed and carefully consider privacy and confidentiality in the acquisition process. Avoid acquiring sensitive data unless absolutely necessary; one of the best ways to reduce confidentiality risk is to reduce the amount of sensitive data being collected in the first place. Confidentiality risk can be further reduced by using sensitive data only as approved and as necessary.

Manage devices

Computer management is a broad topic that includes many essential security practices. By protecting devices, you can also protect the data they contain. Follow basic cybersecurity hygiene by using anti-virus software, routinely patching software, whitelisting applications, using device passcodes, suspending inactive sessions, enabling firewalls, and using whole-disk encryption.

Contact Information

Compliance Comitee

The Compliance Comitee is available to answer any questions about the Code or Company compliance policies, or to discuss any concerns you may have about potential Code violations through confidential and safe channel on www.atria.arq.br. Visit "Compliance"menu.

General Contact

+55 61 3443-8654

info@atria.arq.br

Address:
SCLS 208 BLOCO C LOJA 34
Asa Sul, Brasília - DF, Brazil
70.254-530

Appendix 1

Security information compliance term

Security Information Compliance Term

Confidentiality

Name:	Document Number:
Company:	Role:
Professional Association:	Contact Number:

I declare to have permission to access the information from ATRIA, or under its responsibility, necessary for the performance of the activities performed to the company contracted by ATRIA, in which I am linked, and I commit to comply with the provisions of the following items:

1. Have knowledge and strictly comply with all ATRIA policies and procedures regarding information security.
2. Be aware that the accesses referred to in this document have been granted for exclusive use in the activities for which they are intended.
3. Observe the classification of the information to which it has access, according to the criteria established by ATRIA according to the activities performed by me.
4. If necessary, when disclosing information from ATRIA, observe the established criteria.
5. Do not use my access to visualize unnecessary information or data for the exercise of my activities.
6. Do not use my accesses to copy or remove computational resources, information owned by or managed by ATRIA, without specific authorization for that purpose.
7. Do not use my accesses to interfere with services, causing, for example, congestion, alteration, slowness, or interruption of ATRIA network traffic.
8. Do not use the resources provided by ATRIA for illegal activities, such as defamation, discrimination, obscenity, pornography, threat, theft, attempted unauthorized access to data or attempted to circumvent security's system protection, interception of electronic messages and breach of Copyright.
9. Do not discuss or quote ATRIA's internal affairs in public, physical or virtual environments.
10. Respect property rights, installing and / or using only authorized technological resources and with the respective licenses with valid users' licenses.
11. Communicate to the contracted party's representative any suspicion or evidence of violation of the rules, especially for cases in which ATRIA's commitment to corporate information is proven or under its responsibility, preventing the Company's image from being put at risk with to its internal and external public.

I am aware that:

- The security's information responsibilities extend beyond working hours and continue even after the employment contract has ended end, for information obtained as a result of the activities performed for the company contracted by ATRIA;
- Failure to comply with any item of this document shall result in the application of the sanctions mentioned in the contract, applicable to the contracted company, and also in other legal and civil and criminal liability cases, also applicable to the service provider agent.

_____ , _____ of _____ _____

Location / Date

_____ _____

Contracted Party Signature

Name, Document's Number and Signature of the Contracting Party 's Representative

Appendix 2

Non-disclosure agreement

Non-Disclosure Agreement

To
_____ (Name of the Company)
ATT.

_____ (Name of the Company's Representative)

Having knowledge of the _____ (Description of the Works) for the _____ (Object of the Works), regarding ATRIA's contract for the project owned by the _____ (Name of the Client), I, _____ (Name of the Company's Representative), _____ (Document Number), declare to be aware and in accordance that no information distributed or shared with _____ (Name of the Company) and its direct or indirect staff, will be disclosed, stored, copied or shared with third parties, by any means, physical or electronic, and under no circumstances or pretext, as stablished in the original note transcribed below:

> *"Transcribe note regarding the document's property and prohibition of distribution"*

It will be imputable in accordance with the Brazilian copyright and intellectual property law, as well as to all the client's sanctions regarding the unauthorized disclosure of information, as per the original note transcribed bellow:

> *"Transcribe note regarding the confidentiality requirements expected from all parties involved."*

_____ , _____ of _____ _____
Location / Date

_____
Name, Document's Number and Signature
of the Company's Representative

_____
Name, Document's Number and Signature
of the Company's Representative Witness