Supplier Evaluation Policy

Category: Legal, Compliance, Governance & Ethics, Operational Risk

October/2021

Objectives of this Policy:

This policy presents the governance and control framework for the assessment, implementation, review, and ongoing management oversight of BTG Pactual's service providers and suppliers. It addresses the controls applicable to those counterparties with whom BTG Pactual intends to engage or already has a relationship.

These are minimum standards and processes applicable to BTG Pactual's entities globally and additional requirements imposed by specific regulation or legislation that must be identified by legal entities where relationships with third party service providers or suppliers exist.

It also requires that all risks associated with any Outsourcing arrangements made by BTG Pactual are properly identified, reviewed and in compliance with all laws, regulations and the minimum standards established by this policy.

Main Related Standards:

- Resolution No. 4,557, of February 2017 - Central Bank of Brazil
- Resolution No. 4,557, of February 2017 - Central Bank of Brazil
- Resolution No. 4,893, of February 2021 - Central Bank of Brazil
- Resolution No. 4658, of April 2018 - Central Bank of Brazil
- Circular Nº 3978, January 2020 - Banco Central do Brasil
- CVM Instruction 505, of September 2011 - Brazilian Securities and Exchange Commission

Key Related Policies:

- L&C 001 - GLOBAL - Code of Business Principles & Ethics
- L&C 005 - GLOBAL - Compliance Manual
- L&C 007 - GLOBAL - Information Barriers
- L&C 021 - GLOBAL - Records Management
- L&C 035 - GLOBAL - Anti-Corruption and Anti-Bribery Policy
- IT 022 - BRAZIL - Data Security, Classification and Lifecycle
- IT037 - GLOBAL - Cyber Security
- COMP 003 - GLOBAL - Corporate Governance - Risk Management & Control Framework
- OR 002 - GLOBAL - Business Continuity Management
- AML 001 - GLOBAL - AML Program
- ESG 001_Sustainability Policy

To whom does it apply?

All employees of all business and operational areas of Banco BTG Pactual and other entities that are part of the prudential conglomerate.

Principles and Associated Controls:

- Designate one person responsible for all outsourcing agreements.
- Perform risk assessments, processes, and controls (Risk Assessment) regarding to the service / function / data to be transferred.
- Establish ongoing reporting and monitoring cycles depending on the risk exposure and materiality of the outsourced/official service/function/data.
- Always involve the Contracts & Procurement department.
- Formalize all outsourcing agreements through a written legal contract (Service Level Agreement) containing appropriate data security / confidentiality clauses.

Summary

CHAPTER 1 - Management of Third Parties

1. Objective and Scope

1.1. Objective

This policy presents the governance and control framework for the assessment, implementation, review, and ongoing management oversight of all outsourced services (e.g. transfer of a service, function, or data) by BTG Pactual. It addresses the controls applicable to service providers.

Establishes minimum standards and processes applicable to BTG Pactual entities globally. Additional requirements imposed by regulation or legislation in specific local jurisdictions must be identified by the legal entities where services are provided.

1.2. Scope

This policy applies to all Outsourcing arrangements made by BTG Pactual acting as an Outsourcing contractor with a Service Provider.

Examples:

Outsourcing: agreement with outsourced company for external storage of documents. agreement with third-party call center company for registration of customer complaints.

This policy does NOT apply to:

- Customary outsourcing arrangements with financial (or equivalent) institutions subject to the same (or equivalent) laws, rules and regulations as BTG Pactual (e.g.: a custody agreement with another financial institution, an investment management agreement with an asset manager, agreements to engage brokerage firms to trade equities, etc.).

- Outsourcing of services to external legal advisors.

- Intra-group service provision.

NOTE: External legal counsel must be retained by BTG Pactual's Legal Department.

2. Categories of Outsourcing

Non-exhaustive list with examples of activities that will be subject to the requirements of this policy:

- Service provider outsourced by IT (e.g. maintenance and support of BTG Pactual's applications or hosting).
- Software/system outsourced by IT (Software as a Service - SaaS).
- Business Process Outsourcing (e.g. transferring business operations such as payments, settlements or reconciliations, HR, accounting and payroll to an external service provider in another country).
- Outsourcing of knowledge processes (e.g. hiring a third party in a foreign country to produce research for BTG Pactual).

Outsourcing agreements entered by BTG Pactual's Entities are, in principle, the responsibility of the respective Entity/Business Group.

3. Requirements for Outsourcing

3.1. Minimum Required Standards

The use of third parties to perform internal processes, sometimes supporting critical processes, requires a thorough assessment of the potential risks that their operations could generate for Banco BTG Pactual. Therefore, we must carefully consider the best ways to manage and minimize exposure to these risks. Each Business Unit defined as responsible for outsourcing must exercise due diligence throughout the outsourcing life cycle from the beginning to the end of the contract.

To meet the minimum standards set forth in this Policy, business functions must consider each Outsourcing contract individually, considering the following factors:

a. Relevant legal and regulatory requirements (including, where necessary, approval from regulators and customers).
b. The materiality of the data/service/function to be transferred outside the company and/or outside the country.
c. The level of control to be exercised by the Responsible Outsourcing Contractor over the Service Provider.
d. The governance structures necessary to mitigate risks and to ensure oversight and management of the Outsourcing agreement by the responsible Contractor.

3.2. Contract Responsible

The Business Unit responsible for the Outsourcing contract must designate a contract responsible, that must have the seniority, experience, and knowledge commensurate with the importance of the Outsourcing contract. He / she must obtain approval of the proposed arrangement from the head of the area and, in addition, must control and monitor the Outsourcing contract throughout its useful life, from start to final operation.

In certain jurisdictions, responsibility for outsourcing arrangements must rest with a person approved by the relevant regulator. The determination as to whether their appointment must be approved by the relevant regulator must be made by Business Group Legal and Compliance.

3.3. Restrictions

The following functions and provisions may **NOT** be outsourced or outsourced:

- The oversight, monitoring, management and control responsibilities of the Board of Directors and the senior management committees of the Business Group and equivalent bodies of any BTG Pactual Entity.

- Basic management functions, such as defining strategies and policies regarding to BTG Pactual's risk profile and control, supervising, or controlling the operation of its processes.

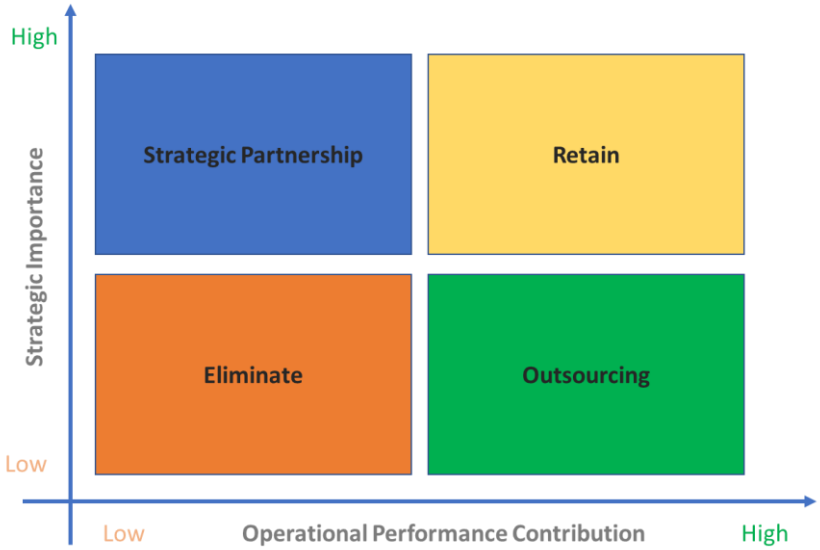
- Any decision regarding the commencement or discontinuation of business or business relationships.

In addition, the service provider may only appoint subcontractors with the specific written consent of the contract owner, the area head, and the Legal and Compliance departments.

4. Contratual Process

4.1. Pre-Contractual Analysis - Responsibilities and Risk Assessment

The Responsible Contractor must expose to the head of its area the criteria for outsourcing, aligned to the outsourcing decision matrix aligned with the best market practices:



After understanding the scope of service to be covered, criteria for the outsourcing decision and the company profile, the responsible forwards the contract to the Contracts & Procurement (C&P) department, which verifies adherence to the minimum clauses required for service and supply providers. Concomitantly, the Onboarding area analyzes the legal history and reputation of the third party. In the client's KYC process (carried out by the Onboarding team or by Compliance), automated search systems are used that consider social and environmental information and consult databases with social and environmental information such as:

- Register of Employers who have submitted workers to slave conditions, published by the Ministry of Economy at the time of contracting the operation ("Slave Labor List of the Ministry of Economy").
- Relation of areas embargoed by the Brazilian Institute for the Environment and Renewable Natural Resources (IBAMA).
- Automated search queries with word combinations of the vendor name with "pornography" "prostitution" "child labor" "slave labor".
- CNAE CTF: list of CNAES subject to IBAMA's Federal Technical Register of Potentially Polluting Activities.

- World Check: tool that verifies the list of sanctions of international environmental agencies (USA, Canada, Colombia.

If a socio-environmental note is identified, the ESG desk will conduct a (manual) analysis and may:

- Approve the relationship without the classification of high socioenvironmental risk.
- Approve the relationship with the classification of socio-environmental risk.
- Disapprove the relationship.

Counterparties classified as high social and environmental risk will be considered those that have lawsuits/media directly or indirectly related to issues involving slave labor and IBAMA embargoes (depending on the type of relationship).

For risk attribution, the sector and location of the counterparty will be considered. For transactions classified as high social and environmental risk, the ESG Head will be responsible for approving the opening of the account, as well as the competent business heads.

In accordance with BTG Pactual's Environmental and Social Risk Policy, we do not enter transactions with individuals or companies that exploit slave labor, understood as those included in the Ministry of the Economy's Slave Labor List.

After these steps, the contract is forwarded to the legal and information security department for specific opinion. After collecting the analyses from all areas involved, C&P makes the information available to the responsible for the contract, which chooses to follow if there are no relevant surveys or looks for another supplier option if the risks found are not in the risk appetite or cannot be mitigated. The Responsible who has contracted service/supply remains fully accountable in relation to that procurement. The area must therefore retain the necessary knowledge to effectively oversee the contracted service/supply and manage the risks associated with the contract.

An area that has outsourced a service / function or data remains fully accountable regarding to that activity / information. The area must therefore retain the necessary knowledge to effectively oversee the outsourced service / function / data and manage the risks associated with the contract.

5. Approval Process

The contract responsible shall ensure that each proposal for an outsourcing contract for a material amendment to an existing outsourcing contract is approved by at least:

- Head of the respective area.
- Compliance.
- All infrastructure areas affected.

Approvals may be incorporated into other procedures or guidelines, for example as part of the Business Group New Business Approval process, Offshoring Business Initiative process or equivalent.

All Outsourcing agreements must be documented in a written agreement, regardless of the level of service or risk associated with the agreement. The agreement must be approved prior to signature by the responsible legal department and, if applicable, by the Finance - Tax area. All agreements related to outsourcing of services must contain data security/confidentiality/anti-corruption clauses approved by the legal department.

The financial arrangements for inter-company transactions must be properly documented and approved by the Finance / Tax area prior to the finalization of the contract.

No legal, financial, moral, or other commitments may be made to the Service Provider, whether in the form of a legal contract (written or oral) or any other document or undertaking, until all necessary approvals have been obtained.

6. Controls and Reporting

6.1. Database

- The Contracts & Procurement area holds a database with minimum information about all outsourced service providers that have already worked for the BTG Pactual group.

- The Internal Controls area holds the list of service providers related to processes mapped with the areas.

6.2. Process Mapping and Incident Reporting

Every third party should be reported to the Internal Controls and Operational Risk areas during process or risk mapping. The contracting area must regularly report all outsourcing arrangements to Operational Risk, to allow the identification, monitoring and evaluation of potentially significant issues. Relevant incidents materialized in the processes carried out by third parties should also be informed to Operational Risk, as well as unavailability or interruption of operations.

The Operational Risk area is responsible for categorizing the third parties as to their level of criticality and then proceed with the appropriate roadmap for each level according to the process listed in chapter 2 of this document.

7. Communications - Legal and Compliance

If any particular Outsourcing arrangement is deemed "critical", either on its own or as an aggregate Portfolio Risk, or gives rise to a warning requirement as a result of a regulatory requirement in any jurisdiction, the Responsible Officer must inform the Area Head and Legal and Compliance of the nature and scope of the proposed outsourcing or outsourcing agreement.

The communication must conform to the regulator's requirements and must be made as soon as possible to allow the regulator to assess and, where necessary, approve the proposal.

8. Contractual Termination

Provision must be made to deal with expected or unexpected termination of a relationship with a service provider and other service interruptions. In particular, the contract owner must plan and implement arrangements to maintain business continuity in accordance with the Group's plan, including ensuring that all contracts are terminated, that no further obligations arise, that all network access is closed and that any property and data is recovered from the service provider. Further obligations regarding to data management will be specified in agreement with established clauses in contract by Security Office.

9. Waivers/Exceptions

Any exception to this policy, including any request for an exception, must be approved by at least the Legal and Compliance Department and the relevant Area Head or, when related to costs, the Cost Committee.

CHAPTER 2 - Management and Evaluation of Third Parties

1. Third Party Management Scope

To conduct the Risk Assessment, the Contracts area shares the suppliers and service providers that are in the process of contracting or contract renewal for analysis by the Third Party Management team, which is made up of the Contracts, Operational Risk, Business Continuity Management, Credit Risk, Security Office and Compliance department. Third Party Management then performs categorization, risk assessment and any contractual adjustments that may be necessary and holds bi-weekly meetings to deliberate on the suppliers and providers that are in the Due Diligence process. All information collected is available in the GRC - risk management software.

2. Supplier Categorization

Supplier categorization can be defined as Level A, Level B and Level C, so that qualification in one of the categories depends on the supplier's compliance with objective criteria specified below.

Level A

A supplier that meets one or more of the following criteria is considered Level A:

- System providers of SaaS (Software as a Service), PaaS (Platform as a Service) and IaaS (Infrastructure as a Service) type, where the right to use the service offered is acquired.
- Business Process Outsourcing (BPO) service providers.
- Suppliers of security products, anti-fraud services and cloud solutions.

Level B

A supplier that meets one or more of the following criteria is considered Level B:

- Suppliers that fall within the scope of Co-Branding strategic contracting.
- Financial institution, or category audited/regulated by the same bodies as BTG.

All Level B suppliers will be referred for Compliance KYP (Know Your Partner) flow, and if required, this may be included in the operational risk assessment.

Level C

A supplier that meets one or more of the following criteria is considered Level C:

- Cloud Infrastructure Provider.

- Market Data Service Providers.
- Corporate Service Providers.
- Telecommunications providers.
- Service providers of Critical facilities.
- Services of consultancy, Bodyshop, Outsourcing and technical support.
- Suppliers who do not fall into categories A or B.

3. Security Office Analysis

3.1. Process Summary

The Security Office is responsible for assessing third parties from the perspective of information security, which is divided into three aspects. The first refers to the analysis of the technological structure of the service provider. The second aspect seeks to evaluate the provider from the perspective of Resolution No. 4893, February 2021, of the Central Bank of Brazil. And finally, evaluation points are raised regarding data protection and compliance with the laws applicable to the theme as LGPD and GDPR.

The supplier assessment process, through the prism of the Security Office, considers all the categories A, B and C mentioned in the previous section. These categories are divided in two scopes, which have specific due diligence questionnaires. Suppliers level A, B and C can receive the due diligence that contains questions about information security structure, data protection controls, Brazilian data protection law (LGPD), and the Brazilian Central Bank's Resolution 4893, February 2021. Suppliers level C that provide services of consulting, Bodyshop, outsourcing, technical support and similar receive the due diligence that requires information about employee background check, security and data protection awareness, and employee's certifications.

3.2. Security Office Evaluation

The classification of third parties is based on the evaluation of Due Diligence previously sent when there is the process of signing or renewing a contract, or even in cases of development of additives for insertion of specific conditions or new clauses to the contract of the third party. Based on the evaluation, two types of risks are defined:

-Risk Due Diligence
-Risk by type of service

3.3. Risk by Due Diligence:

The risk rating by Due Diligence is obtained quantitatively through the answers generated by the third party via questionnaire. Briefly, each question has a certain weight that can vary from 1 to 3, respectively, from low to high risk. According to each answer, detail and evidence presentation, it is possible to determine if the impact of the requirement is mitigated or exposed. For example: if the third party answers a certain question negatively, not meeting the requirement, it is understood that there is a risk exposure. After all answers and their weights are calculated, it is possible to obtain a Due Diligence score and the proper risk classification.

3.4. Risk by Type of Service

A third party, in addition to its risk assessment derived from the due diligence results, also has a qualitative and analytical assessment as to the type of service or product it provides. In this evaluation the risk classification is also defined as High, Medium and Low. The criteria for categorization are:

-High - the supplier performs storage, processing, or treatment of personal data of customers or employees of the bank or has a service with high financial or reputational impact to BTG Pactual.

-Medium - the third party has certain relevance in bank operations that may involve sensitive information.

-Low - the third party has low impact on the bank's operations.

3.5. Suppliers Review

Revision of a vendor evaluation may occur for several reasons, including:

-The period defined by the Security Office since the last assessment has been completed . This period is usually 12 months.
-A new demand has arisen, on the part of BTG Pactual, and a new service or product from the supplier will be contracted, and some structural or regulatory impact will occur with regard to information security.
-Renewal or extension of the contract already established between the parties, being that the last evaluation may not have reached its maximum period according to the first objective cited above.

Another possibility of reviewing the evaluation of a particular supplier occurs in the short term when the answers and evidence reported are not sufficient for the analysis of the maturity of service provision.

3.6. Contractual Clauses

After the supplier evaluation process, the risk definition, either by Due Diligence or Service Risk, and a possible review due to unsatisfactory answers, the clauses referring to data protection and Resolution 4893 forwarded to the Contracts & Procurement area.

4. Operational Risk Analysis

All suppliers categorized as Level A, will go through the operational risk assess that, in contact with the responsible department, will measure the impact aspects regarding the scenario listed below:

4.1. Operacional Impact

- Low - Slight impact on the schedule of activities. Activities can be recovered in the short term without affecting the normal flow of operation.
- Moderate - Moderate impact on the work schedule such that processes and / or activities must be rescheduled to be able to normalize the normal flow of operation.
- High - Significant delay in the execution of tasks and activities due to workload accumulation. It is necessary to formalize the situation and obtain or request assistance from a third party to normalize the normal flow of operation.

4.2. Regulatory Impact

- Low - May generate a warning and/or monetary fine by regulatory and external inspection agencies for non-compliance with laws and regulations.
- Moderate - May generate internal sanctions for non-compliance with regulations.
- High - May generate, in addition to a warning and/or fine, other administrative sanctions, such as suspension and/or temporary or permanent disqualification from holding management positions in the administration or management for non-compliance.

4.3. Reputation Impact

- Low - Insignificant image impairment.
- Moderate - Does not harm the organization's image.
- High - Impairment merits attention and corrective action.

4.4. Financial Impact

- Low - Does not generate relevant financial impacts for the area.
- Moderate - May generate relevant financial losses for the area.
- High -May generate financial losses significantly impacting the PnL of the area.

The final risk score of this assessment considers the highest risk level of the impacts presented above. And the third parties classified as "High" impact will be included in the residual risk analysis process presented in the next topic.

5. Residual Risk Assessment

In the residual risk stage, third party management requests the supplier to fill out the forms (BCM and CRC), send the policies and additional evidence when necessary. From the answers collected, certain contractual clauses are specified, and the risk level and date of the Due Diligence review is stipulated and registered in the GRC - operational risk system, for shared follow-up.

5.1. BCM (Business Continuity Management) Assessment

Based on the answers collected in the BCM form, which has questions on Infrastructure, governance and good practices, the risk rating is assigned according to the following scale:

Low	If 6 or 5 of the governance responses and 4 of the infrastructure responses were positive.
Medium	Only 3 or 4 of the governance and 3 of the infrastructure responses were positive.
High	Only 1 or 2 of the governance and 1 infrastructure responses form positive.

5.2. CRC Assessment

To define the credit risk score, we request the financial statements for the last three years and analyze the main indicators. The classification is attributed according to the levels below:

Low	Company with recurring revenue history, little doubt, operating cash generator, with track record and well-formed captable.
Medium	Company with tested product, with scale, still burning operating cash, but close to breakeven, has already gone through relevant funding rounds.
High	Early stage company, BTG as one of the first clients, product not yet scalable, burning operating cash, has not been through relevant funding rounds.

6. ESG Charter of Critical Suppliers

Suppliers classified as critical during the operational risk and residual risk assessment stage will receive the ESG Charter for Critical Suppliers which makes reference to the ESG Conduct Manual for Critical Suppliers that contains the recommendations of best practices in terms of sustainability and may be accessed at the following link.

Periodically, critical suppliers must submit the information below. As a result, the best rated suppliers will be mentioned on BTG Pactual's website.

- Realization of the Sustainability Policy Training
- Membership of the Global Compact
- Prioritizing the SDGs
- Carrying out a GHG inventory

7. Third Party Monitoring

Third-party monitoring occurs according to the nature of the service provided. Below are some of the possibilities.

Status page

Third Party suppliers, which provide solutions implemented in their infrastructure, has web status page containing information about service/solution availability and eventual incidents.

API

When a third-party supplier provides a solution through API it is possible to monitor such solution via proxy. In case of solution’s unavailability, the monitoring will be triggered.

Security tools

Security Office’s Cyber Defense Center has specific tools that monitor third-party solutions implemented in own infrastructure (cloud or on-premises). The monitoring consists of log collection.

Incidents
Incidents caused by Third Parties must be reported by the responsible business line to the operational risk team, which will assess the risks and control failures, the impact caused, action plans and record the event in the risk management software.

8. Third Party Issue Management

The steps of Identification, Assessment and Monitoring follows a logic-sequential process, whose key processes identify and assess risks and controls that may demand the development and implementation of Actions Plans to reduce the risk exposure to acceptable levels or its acceptance with a proper rationale and dully approved.

The vehicle used to formalize the outcome of the decision making in the Risk Response is the Issue, where the key information over the exposure/deficiency is described and the action plan/review date or risk acceptance is defined.

All formalized Issues are recorded and have its actions plans followed through closure by Operational Risk and Security Office and reported in internal committees.

APPENDIX A

Clauses – Operational Risk/BCM

I. Aiming to contribute to best practices of Business Continuity, the Contracted Party undertakes to provide, when applicable and requested, the list of business processes hired and the infrastructure associated with each of them, such as the respective messaging systems, APIs, etc. This list will be used to monitor the availability levels of each service. This information must be sent within one month after the signing of the contract and requesting. In case of any changes within the term of the contract, BTG Pactual's operational risk area must be informed.

II. Without prejudice to the other guarantees and obligations assumed in the Contract and for services providers considered critical to the contracting party, the supplier attests to have infrastructure and risk management processes appropriate to its size, risk profile, business model, the nature of its activities and the complexity of the services, in order to ensure the continuity of the services provided, having at least one operational continuity plan and a disaster recovery plan of minimum annual update.

III. Nevertheless, the Contracted Party shall be responsible for the veracity of the documents and business continuity strategy shared with BTG Pactual, undertaking to keep the Contracted Party updated of any significant change in its management process, and making available to the Contracted Party, whenever requested, documents and information regarding its operational risk management structure and compliance therewith, in accordance with Central Bank of Brazil Circular No. 4,557/2017.

Clauses - SO

I. The PARTIES hereby declare to know, agree and comply, without any reservations, with the following provisions regarding the treatment of personal data, considering the provisions of Law 13.709/2018.

II. If there is access, receipt, processing, transmission, treatment and/or international transfer of personal data, due to and in the performance of its activities, related to the present contract, the Parties shall:

a. Comply with data privacy laws in relation to the processing of personal data subject to the Agreement, to the extent applicable.

b. Process the personal data to which it has access due to the provision of the services, with the sole purpose of providing the services for which it has been hired, always in accordance with the criteria, requirements and specifications provided for in the Contract and its respective attachments, without the possibility of using such data for a different purpose

c. Not to disclose to third parties the personal data to which it has had access, except with the prior and express authorization of the other Party.

d. Keep in absolute secrecy all personal data and information that has been entrusted to him, an obligation that will subsist at the end of the Contract.

e. Not to process personal data at a location other than that established by the Parties.

f. Not retain any Personal Data for a period longer than necessary for the performance of the services and/or for the fulfillment of its obligations under the Contract, or as necessary or permitted by applicable law. Upon termination of the Agreement for any cause, the Parties shall securely delete/destroy (upon prior request), or return to the Party that collected the data, all documents containing Personal Data to which it has had access during the provision of the services, as well as any copy of these, whether in documentary or magnetic form, unless its maintenance is required or ensured by applicable law.

g. Collaborate with each other to ensure full compliance with the provisions set forth in the personal data protection laws.

iii. For purposes of this Agreement, "personal data" means all information accessed or received by either Locaweb or Locaweb in any tangible or intangible form regarding, or that personally identifies or makes identifiable, any employee, customer, agent, end user, supplier, contact, or representative of Locaweb.

iv. For purposes of the provisions of item g of clause (ii), the PARTIES shall:

a. Take reasonable steps to inform your staff of the responsibilities and trustworthiness resulting from the Personal Data Protection Act.

b. Notify within 5 (five) to the other PARTY in writing whenever it has knowledge of the occurrence of a security incident, or a violation of the personal data protection law.

c. Investigate any security incident, taking all necessary steps to eliminate or contain the exposure, including cooperating with investigation and remediation efforts, mitigating any damage.

d. Use reasonable efforts to ensure that personal data is correct and up to date in all circumstances while in your custody or under your control, to the extent that you have the ability to do so.

e. Reasonably cooperate with the CONTRACTOR in defining a solution to implement the new requirements of protection and security of personal data, should the legislation so require.

v. Allow the CONTRACTOR, or its duly authorized representatives, provided reasonable notice, to inspect and/or audit its systems, by sending documentation, conducting evidentiary tests, or if so preferred by the audited PARTY, through the evaluation of an independent audit, specialized in the theme, chosen by agreement between the PARTIES, and the agreement of the SERVICE PROVIDER shall not be unjustifiably withheld, to verify and evidence if its activities are in conformity with the provisions of the Contract and its annexes, if any. The CONTRACTOR shall exclusively bear the costs of such inspections or audits.The CONTRACTED one reserves the right to limit the scope of the audit, not being allowed to the CONTRACTOR and/or third parties designated for the audit, to have access to any documents and/or information of the CONTRACTED one that are not related to this Contract.Locaweb may further require that such audits (a) be preceded by advance notice of not less than fifteen (15) days prior to the date scheduled for commencement. (b) be subject to appropriate confidentiality and non-disclosure provisions, and (c) not disrupt the normal operations of Locaweb.

vi. Locaweb further agrees to respect the security measures implemented by Locaweb, including commercially reasonable and appropriate physical, technical and organizational security measures, which are necessary to guarantee the security, confidentiality and integrity of the personal data, as well as with the purpose of avoiding eventual alteration, loss, treatment or unauthorized access in accordance with the provisions of the Agreement and applicable legislation.

OBLIGATIONS AND RESPONSIBILITIES OF THE CONTRACTOR

1.The CONTRACTED PARTY undertakes to:

(...)

i. Define procedures and controls for prevention and treatment of incidents relevant to the contractor.

ii. Notify the CONTRACTING PARTY, within a maximum period of 72 hours, of relevant incidents and their due treatment via OL-SecurityGovernance@btgpactual.com. The CONTRACTED PARTY shall consider a relevant incident as one that compromises the confidentiality, integrity or availability of the service provided or product, that has a financial impact or damages the privacy of the client or the CONTRACTING PARTY's employees.

iii. Hold and grant access to certifications relevant to the service it provides.

iv. Grant access to reports prepared by an independent specialized auditing firm.

v. Provide adequate information and resources for monitoring the services provided.

vi. Have physical or logical controls for the identification and segregation of the contractor's data.

vii. Inform the countries and region (in each country) where the services may be provided and the data may be stored, processed and managed.

viii. Inform about security measures adhered to for data transmission and storage.

ix. In case of contract termination, to carry out the return transfer and deletion of the contractor's data.

x. Notify the contractor of the subcontracting of relevant services.
xi. Keeping the contracting party informed of any limitations that may affect the provision of services or compliance with legislation.

xii. Allow regulators access to the contracts and agreements signed for the provision of services, to the documentation and information concerning the services provided, to the data stored and information on their processing, to data and information backup copies, as well as to data and information access codes.

ESG Clauses

The CONTRACTED PARTY undertakes to:

Remain in compliance, in all relevant respects, with applicable environmental and social laws, regulations, and environmental permits, and states that there are no circumstances that could reasonably support a social or environmental action against you under any environmental or social law.

Remain in good standing with the environmental, occupational health and safety, and other regulatory agencies during the term of this contract.

Respect and support the protection of internationally recognized human rights.

Ensure its non-participation in violation of the rights mentioned above, declaring that it does not encourage and will not encourage prostitution, nor does it use or use illegal child labor and/or in a condition analogous to slave labor during the term of this contract.

Ensure that it performs the management and monitoring of its suppliers and/or service providers, obliging them to perform their activities in accordance with the applicable social and environmental legislation, which includes, but is not limited to, the service provided by its suppliers and/or providers of services of the same obligations imputed to the CONTRACTOR provided for in this clause.

Considering the disposition of the National Policy of Solid Waste, the SERVICE PROVIDER is obliged to collect in the EMPLOYER's facilities and give the destination and/or disposal environmentally adequate to the equipment and/or materials object of this Contract, when requested by the EMPLOYER. Such destination will be done without cost to the EMPLOYER, being the EMPLOYER exempt from any civil, administrative and/or penal responsibility in case of eventual environmental damage caused by the inadequate management of the residues and rejects proceeding from this Contract.

After having identified a volume that justifies the removal of the waste/rejects, the CONTRACTING PARTY will request the removal of these objects by email, informing the address where the removal should occur. The SERVICE PROVIDER will have a period of up to 20 (twenty) calendar days to carry out the removal.

The SERVICE PROVIDER shall send to the e-mail OI-esg-fornecedores@btgpactual.com, at least quarterly, a report of the collections made, specifying the place of collection, date, quantity of waste/waste collected (in units or kilograms) and proof of the destination/disposal of this waste/waste. The CONTRACTED PARTY declares that it possesses all the licenses and/or environmental authorizations necessary for the adequate management of the waste/rejects removed, especially with regard to storage, transport, treatment and final disposal/environmentally adequate disposal.

The CONTRACTED PARTY declares that it will dispose of the removed waste/rejects in an environmentally adequate manner, observing the applicable operational norms in order to avoid damages and/or risks to public health and safety, besides minimizing the adverse environmental impacts.

The CONTRACTED one shall assume any responsibility for the inadequate management of the removed residues/rejects, besides compensating the CONTRACTOR for any amount that the CONTRACTOR is compelled to pay due to the inadequate management, either by way of damage or social and environmental loss, including related to its image.