1. OBJETIVO

We acknowledge the importance of the security, privacy, and confidentiality of the personal information that our users, clients, suppliers, employees, and applicants provide to our Companies through the diverse communication channels available (including websites, apps, and physical documents, among others), and we are committed to their protection and proper processing in accordance with the legal regime for data protection applied to each region we operate in.

2. ALCANCE

Therefore, the Policy scope is to communicate users, clients, suppliers, employees, and applicants, who own such personal information, the type of data and the purpose of the processing to make our provision of service feasible, the protection and the rights that assist them as information holders, and the procedures to exercise them.

This policy applies to all the countries where OneLink provides their services, at an internal level in all administration, management, coordination, and every process throughout the company.

3. DEFINICIONES

- **AUTHORIZATION:** The expressed, informed, and prior consent from the holder to carry out the processing of their personal data.
- **DATA BASE:** An organized set of personal data that is subject to undergo processing according to the law.
- **FILES:** A set of documents kept by the company where information regulated by the law is featured.
- **PERSONAL DATA:** Information that is linked or may be associated to one or several determinate or determinable natural individuals.
- **SENSITIVE DATA:** Those that affect the holder's intimacy or, if misused, can lead to discrimination; such as, those who reveal ethnicity or racial origin; political orientation; philosophical or religious beliefs; participation in unions, social organizations, or human rights associations; and data related to their health, sexual life, and biometric data.
- **HABEAS DATA:** It is the constitutional right that all individuals have to know, update, and rectify the information that has been collected from them at data bases, and the remaining rights, liberties, and constitutional guarantees related to the collection, processing, and circulation of personal

data.

- **PROCESSING PERSON IN CHARGE:** The natural or legal person in charge of the personal data processing on behalf of the company.
- **PROCESSING RESPONSIBLE PERSON:** The natural or legal person that decides upon the bases and the data processing.
- **THIRD PARTY:** Any natural or legal person different from the individuals that belong to OneLink Group.
- **DATA HOLDER:** The natural person whose personal data undergoes processing.
- **DATA TRANSFERENCE:** Data transference happens when the responsible and/or responsible person in charge of the personal data processing at OneLink sends the information or the personal data to a receptor who, at the same time, is responsible for the processing and is located in or outside the country.
- **TRANSMISSION:** The personal data processing that implies the communication inside or outside the territories where OneLink offers their services, when it aims at the performing of a data processing by a person in charge of such processing on behalf of the responsible person.
- **PROCESSING:** Any operation or set of operations about personal data such as recollection, storage, usage, circulation, or elimination.

4. CONDICIONES INICIALES

N/A

5. POLICY INQUIRY

OneLink makes this policy available to all personal data holders at their corporate website, www.onelinkbpo.com.

6. ONELINK GROUP DATA PROCESSING AND PRIVACY POLICY

6.1. LIABILITY

Processing Responsible: The Companies Phone number: + 57 4 444 38 20
E-mail: protecciondedatos@onelinkbpo.com

6.1.1. AUTHORITY

Corporate Security Direction

6.1.2.WHO ARE WE? - THE COMPANIES

COLOMBIA.

ONELINK S.A.S NIT 900964443-0, Aventura Shopping Mall, 7th Floor, carrera 52#65-61, Medellín, Colombia.
GETCOM COLOMBIA S.A.S NIT 900596020-1, Niquía Station Shopping Mall in Bello, 6th Floor, Medellín, Colombia.
GETCOM SERVICIOS S.A.S NIT 900.733.568-1 Niquía Station Shopping Mall in Bello, 6th Floor, Medellín, Colombia.

EXPERTS COLOMBIA S.A.S NIT 900801459-9, Aventura Shopping Mall, 7th Floor, carrera 52#65-61, Medellín, Colombia.

NICARAGUA.
ONELINK NICARAGUA S.A. RUC J031000251843, Rotonda El Periodista 300 meters South, Ofiplaza El Retiro, Building # 6, 3rd Floor.
XPERTS NICARAGUA S.A. RUC J0310000301115, Rotonda Cristo Rey 150 meters West, Juan Pablo II Track.

EL SALVADOR.
GETCOM S.A. DE C.V. NIT 0614071175-002-8, Los Próceres Blvd. and Avenida infantería, Colonia José Manuel Arce, GETCOM Building, San Salvador, El Salvador.
ONELINK S.A. DE C.V. NIT 0501140514-101-9, Torre Cuscatlán Blvd. Los Próceres and Av. Albert Einstein, 7th Floor. TETEL S.A. DE C.V. NIT 0501180614-101-1, Torre Cuscatlán Blvd. Los Próceres and Av. Albert Einstein, 7th Floor.

GUATEMALA.
ONELINK SOLUTIONS GUATEMALA S.A. NIT 90019253, 44 Calle 2-00 colonia Monte María 1 zone 12.
INVERSIONES EXPERTS GUATEMALA S.A. NIT 87451123, 44 Calle 2-00 colonia Monte María 1 zone 12.

MEXICO.
ONELINK SERVICIOS S.A DE C.V RFC: OSE180514FS7 Av 4338, jardines del Pedregral de san Ángel, Coyoacan. ONELINK MÉXICO S.A DE C.V RFC: OME180514IG2 Av 4338, jardines del Pedregral de san Ángel, Coyoacan

6. 2. PRIVACY POLICY CONSENT AND DATA PROCESSING PURPOSES

For the purpose of this policy, "Processing" is understood as any operation or set of operations about personal data such as recollection, storage, usage, circulation, or suppression of such data.

The consent to this Privacy Policy and Personal Data Processing, according to its terms, happens when the user, client, supplier, employee, or applicant provides their personal data through any of the channels or means of communication established by THE COMPANIES.

When accepting the Privacy Policy, each one of our users, clients, suppliers, employees, or applicants, as information holders, authorize THE COMPANIES to perform the data processing in a total or partial manner; including the collecting, storage, recording, usage, circulation, processing, suppression, transmission, and transference inside the country and/or third party countries, according to the terms established at the current Privacy Policy and for the data processing purposes described in this document, especially to:

- Use the received information aiming at the marketing of its own products and services, as well as those of third parties for which THE COMPANIES keep a business relation with, depending on the region where the processing is performed and their regulations.
- Supply the information and personal data to the control and surveillance, administrative, police and legal, national and international authorities in virtue of a legal or regulatory requirement; and/or use or disclose this personal information and data in defense of THE COMPANIES, their clients, our websites or their users' rights, and/or their property to detect or prevent fraud in order to prevent, detect, apprehend, or prosecute criminal offenses.
- Allow the access to personal information and data to the auditors or third parties hired by THE COMPANIES to perform internal or external auditing processes related to the business activities carried out by the Organization.
- Check and update the clients and users' information and personal data in the development of the business activities carried out by the companies.
- Hire third parties to store and/or process the personal information and data for the proper execution of contracts made with us under the internal, legal and regulatory, security and confidentiality standards to which we are obliged.
- Transfer their information and their personal data to the new entity in control of THE COMPANIES or the business unit in case of control change from one or more of THE COMPANIES or any of the business units through merge, acquisition, bankruptcy, split, or creation. If there is a change in the person responsible for the data processing because of the control change, such situation will be informed to the personal information and data holders so they can exercise their rights according to the applicable law. The conditions in which the holders can exercise their rights will be indicated at the moment of reporting the control change.
- Handle the personal information for the proper management of all the processes related to Human Resources within the companies as well as for sending the related information to those processes such as: promoting the verification and evaluation of applicants in the selection processes at the companies, the control and follow-up of the hiring process, the support and execution of the collective benefits derived from an employment contract.

6.3. PERSONAL INFORMATION AND DATA WE PROCESS

6.3.1.AS A RESPONSIBLE ENTITY

THE COMPANIES can collect personal information and data from users, suppliers, employees, and applicants. Such information may vary depending on the requirements from local authorities, technological facilities, nature of the product and/or service to provide, among others. For such purposes, we can collect the following personal information which can be stored and/or

processed at servers located at computing centers, whether owned by the companies or hired from third parties, located in different countries. Based on the transparency principle, we have created a list of personal data to be processed by the companies:

- General Data for Identification: User, client, supplier, employee, or applicant's name, last name and date of birth, ID number, gender, marital status and/or kinship to minors or disabled people who request for our services, occupation, or profession.
- Location Data: Home and/or personal and/or working email address, nationality or country of residence, nationality and country of residence, personal and/or working land line and mobile phone numbers, current employer and position.
- Sensitive Data: Health, biometric data, including images, photographs, videos, voices and/or sounds, fingerprints that identify or make it possible to identify our users, clients, suppliers, employees, applicants, and/or any individual that is found or transit at any premises where THE COMPANIES have set up pieces of equipment and information, as well as movement control and surveillance in general.

The information and personal data holders will not be obliged to authorize the processing of sensitive data at any circumstance. Notwithstanding the abovementioned, in the cases the information holders supply any sensitive personal data to THE COMPANIES in order to provide the service accordingly, they must explicitly consent for THE COMPANIES to process the sensitive personal data or information as established at the current Privacy Policy.

6.3.2. AS ENTITY IN CHARGE

In virtue of the business operation, THE COMPANIES process their clients' data in their capacity as entities in charge and based on the regulations, policies, and contractual guidelines conveyed by them, as responsible for their consumers' data processing, as well as the compliance of the normative dispositions related to the individuals in charge which are applicable in the corresponding territories. THE COMPANIES count on the necessary security measures to process their clients' data properly in their role as entity in charge according to their clients' policies, and the regulatory guidelines from every country.

The strategy regarding personal data and their processing policies are defined by the responsible areas for Government, Risk, and Compliance (GRC).

CALIFORNIA CONSUMER PRIVACY ACT (CCPA).

According to the established dispositions by the "CALIFORNIA CONSUMER PRIVACY ACT," THE COMPANIES can store or know about personal data or information from California state residents in the USA, by serving exclusively as

"Service Provider" and in accordance with the business relation and their clients' instructions. THE COMPANIES do not collect, nor store or process California state residents' data on their own or for their own use or benefit; moreover, THE COMPANIES do not take decisions about the way as their clients deal with or instruct how to process the holders' personal information.

THE COMPANIES count on a scaling matrix to the area or responsible individual designated by their clients to direct the requests regarding personal data processing, including California residents' personal information; consequently, they will refer the data holders to the established channels for the assistance in such requirements by each client.

6.4. PERSONAL INFORMATION AND DATA PROCESSING PURPOSES

6.4.1. GENERAL.

The collected personal information and data are used to process, confirm, comply, and provide the acquired services directly and/or with the participation from other companies or third-party product or service suppliers, promote and advertise our activities and services, conduct business transactions related to payments or charges, comply with legal procedures, fill reports or comply with the requirements from the different national and international control and surveillance administrative authorities, police or legal authorities, banking institutions and/or insurance companies for internal administrative and/or commercial purposes, including market research, audits, accounting reports, statistical analysis, billing, fraud identification, and asset laundering prevention as well as other criminal activities and other purposes indicated in this document.The personal information and data processing, from the responsible entities and the ones in charge, is framed by the guarantee and respect of the processing principles, as defined by the applicable law. These principles are related to lawfulness, legality, liberty, transparency, consent, information, quality, restricted access and circulation, purpose, loyalty, proportionality, security, and confidentiality.

We inform clients, applicants, and users that third parties can be involved in the development of the activities performed by THE COMPANIES, including security tools suppliers for the processing of bank transactions, banking entities, insurance companies, our representatives or agents, and operators. They are also informed that such activities can be provided in countries different from the ones the service has been hired, without limiting other purposes that have been informed in this document, and within the terms and conditions that each one of the products and services from each one of our business units and/or under those third parties' Privacy Policies.

6.4.2. SUPPLIERS

The collected information can be used for the following purposes:

- Carry out evaluations and the selection of potential suppliers.
- Comply with the tax and legal aspects from government and regulatory entities.
- Set business relations to acquire goods or services. Control and pay for the goods and services received.
- Qualitative and quantitative evaluations of the service levels received by the suppliers
- Communication of the policies and procedures regarding the way to do business with the suppliers.
- Control process and accounting record of the duties acquired with the suppliers.
- Consulting, auditing, and reviews derived from the business relation with the suppliers.
- Any other activity necessary for the effective compliance of the business relation between the supplier and the companies.
- Risk lists verification.
- Financial analysis (for those suppliers in which it applies due to the purchase policy).

6.4.3. EMPLOYEES, RETIRED PERSONNEL, AND APPLICANTS

The consent to this Privacy Policy and Personal Data Processing, according to its terms, occurs when the Candidate and/or Applicant, Collaborator hired through an employment contract, linked Third Party, Retired and/or Pensioner collaborator provides their personal data through any channel or any means established by the companies for the correct execution of the different processes and procedures by Human Resources.

As defined in this document, the collaborator and/or the third parties associated through an employment contract, that provide their own personal data and/or from data holders belonging to their family unit and/or their beneficiaries, knows and accepts that the Companies carry out a Personal Data Processing for the purposes intended in this policy by guaranteeing the transparency and compliance of the actual regulations and the Organization's internal policies. When the Collaborator and/or third parties associated through an employment contract act through representation or stipulation in favor of another or by other, it is understood that it is performed under the principle of good faith.

When accepting this Privacy Policy, and at the moment of signing the consent at the contract signing, each one of the information Holders (including the ones from the family unit and/or beneficiaries from the Collaborator associated through an employment contract) authorizes that the Companies partially or totally perform the Processing of their personal data, including its collection, storage, usage, circulation, recording, processing, delivery, and/or national

and international transference and only for the purposes hereby described.

6.5. PERSONAL INFORMATION AND DATA PROCESSING VALIDITY

The validity of the information depends on its purpose compliance; therefore, the information provided by the users, clients, suppliers, employees, or applicants can be stored for up to ten (10) years following the date of the latest data processing for us to comply with the legal and/or contractual obligations they are responsible for especially in accounting, fiscal, and tax matters or for the time needed to deal with the dispositions applicable to any of such matters: the administrative, accounting, fiscal, legal, or historical aspects of the information or in any event as expected by the law and the provision of service.

6.6. INFORMATION RELIABILITY

The users, clients, suppliers, employees, and applicants must provide truthful information to the COMPANIES in order to formalize the reservation and to make it feasible to provide the hired services as well as for any other services required.

THE COMPANIES assume the truthfulness of the information provided by the users, clients, suppliers, employees, and applicants and will not assume the obligation to check the reliability of the users, clients, suppliers, and applicants' identity, nor the truthfulness, validity, sufficiency, and authenticity of the data provided by any of them. Therefore, the companies will not assume any liability for any damages of any nature resulting from the lack of truthfulness, validity, sufficiency, or authenticity of the personal information and data, including damages resulting from homonymy or identity theft.

6.7. PERSONAL INFORMATION AND DATA PROTECTION, SECURITY, AND CONFIDENTIALITY

The personal information and data protection, security, and confidentiality of our users, clients, suppliers, employees, and applicants are of high importance to THE COMPANIES.

THE COMPANIES count on security policies, procedures, and standards which can be modified at any moment whenever they require so as the aim is to protect and preserve the integrity, confidentiality, and availability of the personal information and data, independently from the media or format it is contained in, their temporary or permanent location, or the way they have been transmitted. In that sense, we rely on security technological tools, and we implement security practices known in the industry that include: sensitive information transmission and storage through safe mechanisms such as coding, the use of safe protocols, technological components insurance, information restricted access to authorized personnel only, information backup, safe

practices for software developments, among others.

Every contract signed between THE COMPANIES and third parties (contractors, external consultants, temporary collaborators, etc.) that involve the personal information and data processing of our users, clients, suppliers, employees, and applicants include a confidentiality agreement that describes their commitment to the protection, care, security, and preserve their confidentiality, integrity, and privacy.

6.8. INFORMATION HOLDER RIGHTS

The information Holder is informed about their rights granted by the applicable laws as personal data Holder. Those rights are as follows:

- Know, update, and rectify their information and personal data to the entity responsible for or in charge of their personal information and data processing.
- Request proof of the authorization granted to the responsible entity in charge of the Processing except for when it is explicitly excluded as a Processing requirement.
- Be informed by the entity responsible for or in charge of the Processing, upon prior request, about the use that has been given to the Personal information and data.
- File complaints about infringement to the personal data protection regulation to the competent authorities as applicable.
- Revoke the consent and/or request the elimination of the personal information and data based on the terms presented in this document.
- Access to their personal information and data that has undergone Processing, upon prior request to The Companies, in the current regulatory terms as applicable. For more than one inquiry placed every calendar month, The Companies will charge the shipping, reproduction fees; and if given the case, the certification of documents to the requesting Holder.

6.9. RESPONSIBLE AREA FOR PERSONAL DATA PROTECTION

Processing Responsible: Corporate Security Management.
Phone number: 57 4 444 38 20
E-mail: protecciondedatos@onelinkbpo.com

6.10. GENERAL PROCEDURE FOR THE EXECUTION OF USERS, CLIENTS, SUPPLIERS, EMPLOYEES, AND APPLICANTS' RIGHTS AS PERSONAL INFORMATION HOLDERS.

THE COMPANIES' users, clients, suppliers, employees or applicants have the right to know about the details about their personal data processing and to exercise their rights as their Holders under the applicable data protection terms and as established by the current Privacy Policy.

In order to apply the previous information, the current policy defines the general procedure to exercise the information Holders' rights, unprejudiced of the application of the specific provisions and procedures that local laws can contemplate in every territory. Given any discrepancy within the general procedure and the specific provisions and regulations contained at the local applicable laws in each territory, the specific provisions will prevail.

The Personal Data Privacy area is the one responsible for promoting and enforcing the compliance of the Personal Data Protection Program within the Organization. For this reason, the Organization has enabled specific attention channels for the petitioners to exercise their rights on Personal Data Processing, i.e. the email address protecciondedatos@onelinkbpo.com

If the request is incomplete, OneLink will ask the petitioner to fix the mistakes within five (5) days after the inquiry has been received.

The required information must be presented by the petitioner within the two (2) subsequent months to the request; if not done, it will be understood they have desisted.

The maximum time for OneLink to attend the request is fifteen (15) business days taken from the following day the request was received. If the request is not possible to be attended in that time, the petitioner will be informed about the reasons for the delay and the date they will have their request fulfilled, which cannot exceed more than eight (8) working days following the first overdue deadline.

6. 11. REQUESTS

- The information Holder and/or who acts on their behalf must validate their Entitlement in order to avoid the loss, request, unauthorized or illegal use or access from an individual different from the Petitioner and/or someone who does not have the legal permission to act as such.
- The Holder's validation will be carried out by presenting a physical or digital copy of the relevant ID according to the means by which the request was placed.
- When the request is done by a person different from the holder, the Third party must validate their identity or mandate in the proper way to act on their behalf by sending the supporting documents.
- The request to exercise any of the aforementioned rights must be presented by a physical and/or digital written document through any of the channels enabled by the Organization and that have been identified in the current Privacy Policy for that purpose.
- The request to exercise any of the aforementioned rights must contain at least the following information:
- Petitioner's name, their representative, and/or the person that exercises the

right under their name.
- Concrete, precise, and justified request of the required right.
- Physical and/or electronic addresses for notifications.
- Petitioner's signature according to the means by which the request was placed.
- The request will be managed by the area and/or delegate in charge of personal data protection within the organization only when the Ownership is accredited, and it complies with all the aforementioned requirements.

6. 12. CLAIMS

- The information Holder and/or who acts on their behalf must validate their Entitlement in order to avoid the loss, request, unauthorized or illegal use or access from an individual different from the Petitioner and/or someone who does not have the legal permission to act as such.
- The Holder's validation will be carried out by presenting a physical or digital copy of the relevant ID according to the means by which the request was placed.
- When the request is done by a person different from the holder, the Third party must validate their identity or mandate in the proper way to act on their behalf by sending the supporting documents.
- The request to exercise any of the aforementioned rights must be presented by a physical and/or digital written document through any of the channels enabled by the Organization and that have been identified in the current Privacy Policy for that purpose.
- The request to exercise any of the aforementioned rights must contain at least the following information:
  - Petitioner's name, their representative, and/or the person that exercises the right under their name.
  - Concrete, precise, and justified request of the required right.
  - Physical and/or electronic addresses for notifications.
  - Required documentation to support the request (if it applies).
  - Petitioner's signature according to the means by which the request was placed.
- The request will be managed by the area and/or delegate in charge of personal data protection within the organization only when the Ownership is accredited, and it complies with all the aforementioned requirements.

6. 13. PRIVACY POLICY MODIFICATIONS

We, THE COMPANIES, reserve the right to exercise modifications or updates to this Privacy Policy at any moment for legal developments, internal policies, or new requirements for the provision or offer of their services or products.

These modifications will be available to the public through the following media: visible advertisements in their premises or in our websites, Smartphone applications, or electronic kiosks (Privacy Notice) or via the last provided email

address.

Subject to the applicable laws, the Spanish version of this Privacy Policy will prevail above any other version disclosed in another language. In the event of any inconsistency between this Privacy Policy in its Spanish version or any translation to any other language, the Spanish version will prevail.

6.14. VALIDITY

This General Privacy Policy becomes effective from the day it is published.

7. DOCUMENTOS DE REFERENCIA

- Statutory Law 1581 of 2012 – Personal Data Protection Law in Colombia.
- External Possession of Personal Data Protection Federal Law (LFPDPPP in Spanish) in Mexico.
- Law 787 of 2012 – Personal Data Protection Law Nicaragua.
- General Data Protection Regulation EU 2016/679
- California Consumer Protection Act (CCPA)
- Additional acts, laws, or regulations that modify or add them.

8. HISTORIAL DE CAMBIOS

VERSIÓN	FECHA	RAZÓN DE LA ACTUALIZACIÓN
1	22/Sep/2020	Creation of the policy in english, translation of the spanish version (Política de privacidad y protección de datos personales, GJ-T-R-002) We list the spanish version, as evidence of its existence prior to this version: v1. 206/09/08: Creation of the personal data processing policy. v2. 2017/11/22: Some numerals were modified. v3. 2018/03/15: Re-structuring of the applicable policy to the personal data protection laws where OneLink provides their services. • New applicable laws and regulations are identified and added to the personal data protection. • Incorporating the existing document to the integrated management system. v4. 2018/05/07: A procedure is modified to comply with the ES-GE-Tq-I-01 documentary instruction from the management system. v5. 2019/01/15: A procedure is modified in order to include employees, applicants, and pensioners' data processing guidelines. v6. 2020/02/06: The Corporate Security Director is

		included as responsible user and additional approving officer. v7. 2020/07/07: The segment about the "California Consumer Privacy Act" is included.

ELABORÓ	REVISÓ	APROBÓ
Nombre: NAVIA YURLEY MESA LOPERA **Cargo:** Analista legal **Fecha:** 14/Jul/2020	**Nombre:** LORENA MARIA HOLGUIN MOLINA **Cargo:** Coordinador de estándares y sistemas de gestión **Fecha:** 21/Jul/2020	**Nombre:** FERNANDO MORENO ALVAREZ **Cargo:** director de seguridad corporativa **Fecha:** 31/Jul/2020 **Nombre:** PAOLA ANDREA SAAVEDRA MORENO **Cargo:** Gerente legal **Fecha:** 05/Ago/2020