INTELIGO GROUP

Corporate Guidelines Data Protection

PROCESSES AND QUALITY

www.inteligogroup.com

General Overview

Objective

To establish the treatment for compiling, using, storing, transferring, consulting and protection the Personal Data received voluntarily, directly or indirectly, domestic or international, from the owners of the Customer Personal Data to Inteligo Group and/or any of its Subsidiaries, by, not only the Employees of the Subsidiaries, but also by the suppliers, vendors and providers ("Providers") and, in general, by any third party with access thereto.

Scope

This policy applies to the Areas responsible for receiving, sending and processing the Personal Data of the owners thereof, to which Inteligo Group and/or any of its Subsidiaries have access, as well as such Employees and Providers as may have access to the Personal Data, The Personal Data may be about Customers, Potential Customers, Employees, Providers and, in general, about any third party.

Definition

- **Information Assets:** Information generated processed or received between Inteligo Group and/or its Subsidiaries, used for providing support to or executing business processes and administrative decisions. Examples: files, data bases, system documentation, user manuals, training materials, procedures, continuity plans and others.
- **Consent:** Prior, express, unequivocal and informed expression of the free will, whereby the interested parties indicate their agreement with the treatment of their Personal Data.
- **Personal Data:** Is any information concerning the Owners of the Data that identifies them or makes them identifiable.
- **ARCO Rights:** Inalienable basic rights of the Data Owners, identified as: the Right to Access, Rectification, Cancellation, Opposition and Portability, pursuant to the terms defined in the Personal Data Protection Regulations.
- **Data masking:** Is the process whereby certain elements of the data in a data storage are being changed, changing their information, but with the result that the structure remains similar, so that the sensitive information is protected.
- **Responsible for Consent:** This is the person in charge of requesting, obtaining and processing the consent of the persons for the treatment of their Personal Data, pursuant to the policies and procedures established at each subsidiary, assuring that the consent given is a free, prior, express, unequivocal and informed consent.
- **Transborder Flows:** Inteligo Group and/or its Subsidiaries may send the Personal Data outside their jurisdiction in such cases as may be set forth in their respective Privacy Policies. In most cases, such transborder flows occur towards service providers and/or to some of Inteligo Group's Subsidiaries, for storing, treating or processing the Personal Data. In such cases, Inteligo Group and its Subsidiaries should implement the necessary procedures needed for ensuring that the recipients of the Personal data comply with the Personal data protection regulation and the applicable laws of the country where the processing is being carried out.

- **Recipient of the Personal Data:** This is each and every private law juridical or natural person, including the branches, affiliates, related companies or similar, or public entities that receive the data in the event of a national or international transfer, whether as owner or as person responsible for the Personal Data bank or as a third party. This could be the Inteligo Group or any of its Subsidiaries, providers of external services or professionals (e.g. experts, translators, information service providers, banks, outside consultants or others).
- **An Issuer or Exporter:** Is the owner of the Personal Data bank or such persona as may be responsible for the treatment thereof, located in a jurisdiction, making a transfer of Personal Data to another person or to another jurisdiction.
- **Data Transfer:** This means to inform, disclose, communicate, exchange and/or transmit, in any way and by any means, from one point to another, within borders or trans bordering, data to individuals or entities other than the Owner, whether determined or undetermined.
- **Data Treatment:** Any technical procedure or operation, automated or not, that makes it possible to compile, record, organise, store, preserve, prepare, modify, extract, query, use, block, suppress or communicate Personal Data.
- **Subsidiary(ies):** Is any of the Inteligo Group Corp. subsidiaries, the current ones as well as any such others as may be acquired or set up in future. Currently the Subsidiaries of Inteligo Group are: Inteligo Bank Ltd.; Inteligo SAB, S.A.; Interfondos, S.A. SAF; Inteligo Peru Holdings S.A.C. and Inteligo USA, Inc.

Administration of this Policy

Inteligo Group and its subsidiaries may transfer the data of its Customers, Employees and/or Providers outside its jurisdiction for compliance purposes (e.g. anti-money laundering regulations), for treatment, processing or storage of the Personal Data, be it to other Subsidiaries of Inteligo Group and/or non-related companies, in order to enhance our services and ensure an efficient data processing. Inteligo Group and its subsidiaries may only transfer the data of a Customer, Employee, Provider or third party when they have given their explicit consent thereto and such consent has not been revoked.

Sanctions

Any failure to comply with this Policy by the Employees of any of the Subsidiaries is regulated in their respective Codes of Ethics, internal Code of Conduct, or in the Employee Handbook, while any failure to comply by Providers or third partiers is regulated by their respective Non-Disclosure Agreements.

Information Confidentiality Assurance

General Guidelines:

- Inteligo Group and its Subsidiaries must comply with the rules, regulations and policies for the protection of Personal Data in the jurisdictions where they operate.
- Inteligo Group and its Subsidiaries should ensure a correct treatment of the data banks and also keep a record of each and every creation and/or update of a data bank. In the event that applicable legislation requires the registry or communication of a data bank to some government authority, Inteligo Group and/or its Subsidiaries must comply with such registry or communication.

- Inteligo Group and its Subsidiaries should ensure the ARCO rights to the Personal Data Owners granted to said Personal Data Owners by the legislation that applies in the jurisdiction where they operate.
- Inteligo Group and its Subsidiaries store and process personal information, applying security measures as well as to ensure that they are not lost, abused, accessed, disclosed, altered or destructed inappropriately.
- Data are masked when the information is being used in non-productive applications or environments, electronic back-ups are made and the information is stored in safe places with restricted access.
- The Areas that manage the Personal Data information should keep a record of the staff having access to such information. This should be updated in the event of new hires or leaving staff.
- The Heads of the Areas that manage the Personal Data information should define the roles that will have access to the information.
- Access to Personal Data is only authorised for those that require it for fulfilling their duties in their work.
- Each and every Subsidiary is responsible for assuring the implementation of a control and record of the Employees that have access to the Personal Data banks.
- The Employees, especially the authorised staff, should only use technological devices like PCs, Laptops, Hard Disks and removable media approved by Technology and Information Security.

Responsibilities

1. The Person Responsible for Personal Data at the Subsidiaries should:

- Oversee compliance with these here Guidelines at the Subsidiary where he or she has the role of being Responsible for Personal Data.

2. Authorised Persons are Responsible for:

- Compiling information in the data bases to which they have access in order to be able to manage some service, as set forth in the contractual means as well as the established purposed thereof.

3. The Legal Managers of the Subsidiaries are responsible for:

- Ensuring, through contractual means or through other legal means that those who receive Personal Data are bound to comply with the practices and policies that assure the confidentiality of the data transferred and that they are not going to be used for any other purposes than those previously established.
- Assuring that, in the event of any failure to comply, we proceed to require the person that failed to comply, pursuant to the contractual dispositions or the policies, codes of ethics or the employee handbook of the Subsidiary that they comply with their obligations and in the event that such failure to comply does persist, then the application of resolving the agreement or the application of such penalties as have been previously been contractually established should be evaluated.

4. The Persons in Charge of Obtaining the Consent of the Data Owners are responsible for:

- Requesting the consent from the Personal Data Owners, assuring that such consent is given freely,

expressly, unequivocally and informedly.

- Ensuring the custody of such consents, during the term that the data of the personal Data Owner are being used.

5. The Heads of Human Resources are responsible for:

- Assuring that, in the documents of hiring Employees at the respective Subsidiary it is established that the Personal Data of the Customers, Employees, Providers or third parties should be managed confidentially, even when the contractual relationship with them has been terminated.
- Ensuring that all Employees of the subsidiaries receive constant training about the policies and protocols for confidentiality, data protection and the applicable sanctions, among others, in order to prevent that Customer-related information is shared without the required confidentiality and with unauthorised personnel.

6. The Heads of Information Security are responsible for:

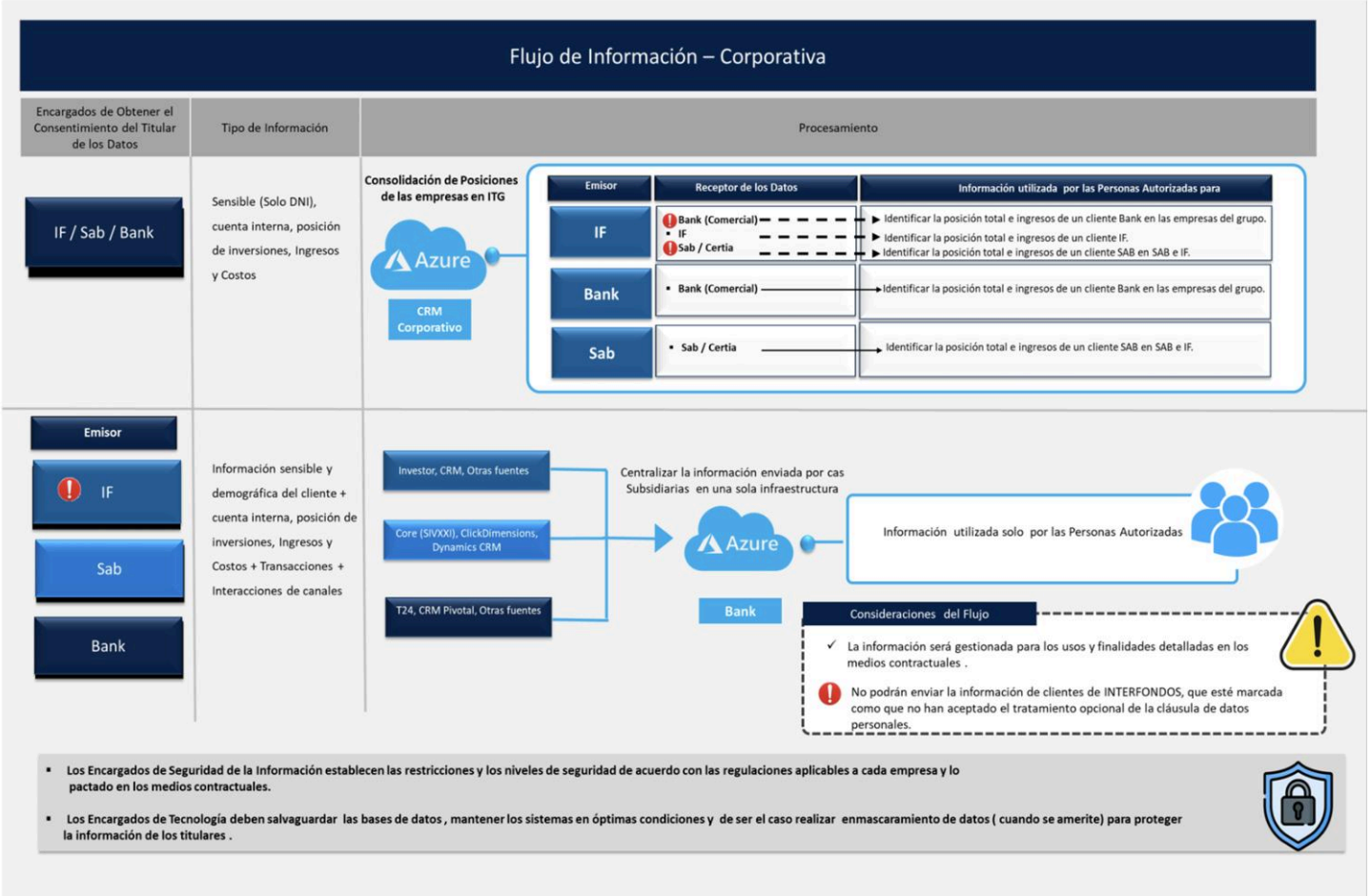
- Ensuring that the systems contain the necessary restrictions and optimal security levels needed for preventing any leak or loss of information.
- Establishing controls that make it possible to check that the Information Assets are duly classified and protected.

7. The Heads of Information and Technology are responsible for:

- Keeping a record of the people that are processing some transfer of data (Copying/restoring of Data Bases).
- Establishing controls for carrying out the destruction of the information when its storage cycle has been fulfilled or whenever some information is no longer required, by secure deletion, if they are on a hard disk or removable device; e.g. memories, USB, CD, solid state drives.

8. The Heads of Auditing are responsible for:

- Monitoring and validating the correct destruction of Information Assets.


Flujo de Información – Corporativa
Encargados de Obtener el Consentimiento del Titular de los Datos
Tipo de Información
Procesamiento
IF / Sab / Bank
Sensible (Solo DNI), cuenta interna, posición de inversiones, Ingresos y Costos
Consolidación de Posiciones de las empresas en ITG
Azure
CRM Corporativo
Emisor
Receptor de los Datos
Información utilizada por las Personas Autorizadas para
IF
Bank (Comercial)
IF
Sab / Certia
Identificar la posición total e ingresos de un cliente Bank en las empresas del grupo.
Identificar la posición total e ingresos de un cliente IF.
Identificar la posición total e ingresos de un cliente SAB en SAB e IF.
Bank
Bank (Comercial)
Identificar la posición total e ingresos de un cliente Bank en las empresas del grupo.
Sab
Sab / Certia
Identificar la posición total e ingresos de un cliente SAB en SAB e IF.
Emisor
IF
Sab
Bank
Información sensible y demográfica del cliente + cuenta interna, posición de inversiones, Ingresos y Costos + Transacciones + Interacciones de canales
Investor, CRM, Otras fuentes
Core (SIVXXI), ClickDimensions, Dynamics CRM
T24, CRM Pivotal, Otras fuentes
Centralizar la información enviada por cas Subsidiarias en una sola infraestructura
Azure
Bank
Información utilizada solo por las Personas Autorizadas
Consideraciones del Flujo
La información será gestionada para los usos y finalidades detalladas en los medios contractuales .
No podrán enviar la información de clientes de INTERFONDOS, que esté marcada como que no han aceptado el tratamiento opcional de la cláusula de datos personales.
Los Encargados de Seguridad de la Información establecen las restricciones y los niveles de seguridad de acuerdo con las regulaciones aplicables a cada empresa y lo pactado en los medios contractuales.
Los Encargados de Tecnología deben salvaguardar las bases de datos , mantener los sistemas en óptimas condiciones y de ser el caso realizar enmascaramiento de datos (cuando se amerite) para proteger la información de los titulares .