

**Manual de Política de Tratamiento
de Datos Personales de Givaudan
Colombia S.A.S.**

Fecha de Publicación: Agosto de 2023
Fecha de actualización: Agosto de 2023
Versión 2

Í N D I C E

1. Introducción
2. Objeto
3. Alcance
4. Destinatarios
5. Normatividad aplicable
6. Definiciones
7. Principios Rectores
8. Tipología de los Datos
 - 8.1. Dato sensible
 - 8.2. Dato Público
 - 8.3. Dato Semiprivado y Dato Privado
 - 8.4. Autorización del Titular
9. Derechos de los niños, niñas y adolescentes
10. Deberes de Givaudan Colombia S.A.S. como responsable y encargado del Tratamiento de los Datos.
11. Finalidades.
12. Derechos de los Titulares de la Información
13. Autorizaciones y Consentimiento
14. Medidas de seguridad de la información
15. Consultas y Reclamos por parte del Titular
16. Contacto
17. Modificaciones de esta política
18. Vigencia
19. Anexos
 - 19.1. Aviso de privacidad
 - 19.2. Bases de datos inscritas en RNBD
 - 19.3. Procedimiento para la recolección, almacenamiento, uso, circulación y supresión de la información personal de los Titulares.

**Givaudan Colombia S.A.S.
Personal Data Processing Policy
Manual.**

Publication date: August 2023.
Date of update: August 2023
Versión 2

I N D E X

1. Introduction
2. Object
3. Scope
4. Addressees
5. Applicable regulations
6. Definitions
7. Guiding Principles
8. Data Typology
 - 8.1. Sensitive Data
 - 8.2. Public Data
 - 8.3. Semi-private Data and Private Data
 - 8.4. Data Holder's Authorization
9. Rights of children and adolescents
10. Duties of Givaudan Colombia S.A.S. as Data Controller and data processors.
11. Purposes.
12. Rights of the Data Holders
13. Authorizations and Consent
14. Information Security Measures
15. Inquiries and Claims by the Data Holder
16. Contact
17. Modifications to this policy
18. Validity
19. Annexes
 - 19.1. Data privacy
 - 19.2. Databases registered with RNBD
 - 19.3. Procedures for the collection, storage, use, circulation, and suppression of the personal information of Data Holders.

<p>19.4. Gestión de incidentes de seguridad en el tratamiento de datos personales</p> <p>19.5. Políticas y procedimientos orientados a atención de PQR</p> <p>19.6. Política general de seguridad y privacidad de la información.</p>	<p>19.4. Management of security incidents in the processing of personal data.</p> <p>19.5. Policies and procedures oriented to PQR attention</p> <p>19.6. General information security and privacy policy.</p>
---	--

1. Introducción

Givaudan Colombia S.A.S. (en adelante “La Empresa”), es una sociedad por acciones simplificada, constituida legalmente mediante la legislación colombiana, debidamente inscrita en la Cámara de Comercio de Bogotá D.C., cuyo domicilio social es en la carrera 98 No. 25G - 40. Sociedad que se identifica tributariamente bajo el NIT 830.077.389-1 y para los efectos de esta Política se denominará como “La Empresa”

Por mandato legal se establece el tratamiento que se debe realizar sobre la información personal de todo aquel que tenga relación con La Empresa, bajo ese entendido, en aras de garantizar el derecho constitucional de habeas data, así como la privacidad, la intimidad y el buen nombre de los clientes, proveedores, empleados y contratistas de la misma, bien sean estos activos o inactivos, ocasionales o permanentes, se ha creado para el cumplimiento de las leyes y decretos reglamentarios, el presente Manual, en el cual constan las políticas para el Tratamiento de Datos Personales, a efectos de permitir el adecuado ejercicio y protección de los derechos del Titular de la Información, para que en cualquier tiempo pueda solicitar la corrección, aclaración, modificación y/o supresión de la misma.

2. Objeto

A través de la presente política, se establece (i) Manual de Política de tratamiento de datos personales de **Givaudan Colombia S.A.S.**, (que en adelante será denominada **Givaudan** o **La Empresa**), (ii) procedimiento para la recolección, almacenamiento, uso, circulación y supresión de la información personal de los Titulares, (iii) gestión de incidentes de seguridad en el tratamiento de datos personales,

1. Introduction

Givaudan Colombia S.A.S. (hereinafter "The Company"), is a simplified joint stock company, legally incorporated under Colombian law, duly registered in the Chamber of Commerce of Bogotá D.C., whose registered office is located at Carrera 98 No. 25G - 40. Company that is identified for tax purposes under the NIT 830.077.389-1 and for the purposes of this Policy shall be referred to as "The Company".

By legal mandate, the treatment that must be performed on the personal information of anyone who has a relationship with The Company is established, under that understanding, in order to guarantee the constitutional right of habeas data, as well as privacy, intimacy and the good name of customers, suppliers, employees and contractors of the same, whether active or inactive, In order to comply with the laws and regulatory decrees, this Manual has been created, which contains the policies for the Processing of Personal Data, in order to allow the proper exercise and protection of the rights of the Owner of the Information, so that at any time he/she may request the correction, clarification, modification and/or deletion of the same.

2. Object

This policy establishes the Personal Data Processing (i) Policy Manual of **Givaudan Colombia S.A.S.**, (hereinafter referred to as **Givaudan** or **the Company**), (ii) Procedures for the collection, storage, use, circulation, and suppression of the personal

(iv) Políticas y procedimientos orientados a atención de PQR y (v) Política general de seguridad y privacidad de la información.

Este Manual ha sido elaborado de acuerdo con los lineamientos señalados en la normatividad aplicable y vigente sobre la materia; y tiene por objeto dar la información necesaria y suficiente a los diferentes grupos de interés, así como establecer los lineamientos que garanticen la protección de los datos personales que son objeto de tratamiento a través de los procedimientos de **Givaudan Colombia S.A.S.**, para de esta forma, dar cumplimiento de la ley, políticas y procedimientos de atención de derechos de los titulares, criterios de recolección, almacenamiento, uso, circulación y supresión que se dará a los datos personales.

Givaudan Colombia SAS adhiere a esta política, a su vez, de manera integral las siguientes políticas globales de tratamiento de datos personales:

- Data Subject Rights Requests Policy
- Global Privacy and Data Protection Policy
- Global Employees and Contractors Privacy Notice
- Global Picture and Video Management Policy
- Personal data Protection Guidelines for Marketing and Communication teams.
- Personal Data Breach Handling Policy and Procedure
- IM&T Security Policies

3. Alcance

Dar un trámite expedito y legal a las diferentes solicitudes y reclamaciones hechas por los Titulares de la Información, así como por sus causahabientes u otra persona que cuente con la debida autorización. Dar cumplimiento a las exigencias de la normatividad vigente en materia de Protección de Datos

information of Data Holders, (iii) Management of security incidents in the processing of personal data, (iv) Policies and procedures oriented to PQR attention and (v) General information security and privacy policy.

This Manual has been prepared in accordance with the guidelines set forth in the applicable and current regulations on the subject; and aims to provide the necessary and sufficient information to the different stakeholders, as well as to establish guidelines to ensure the protection of personal data that are subject to processing through the procedures of **Givaudan Colombia S.A.S.**, in order to comply with the law, policies and procedures for the attention of the rights of the owners, criteria for collection, storage, use, circulation and deletion that will be given to personal data.

Givaudan Colombia SAS adheres to this policy, in turn, in a comprehensive manner, the following global personal data processing policies:

- Data Subject Rights Requests Policy
- Global Privacy and Data Protection Policy
- Global Employees and Contractors Privacy Notice
- Global Picture and Video Management Policy
- Personal data Protection Guidelines for Marketing and Communication teams.
- Personal Data Breach Handling Policy and Procedure.
- IM&T Security Policies

3. Scope

To expeditiously and legally process the different requests and claims made by the Owners of the Information, as well as by their successors in title or any other person with due authorization. To comply with the requirements of the regulations in force

Personales, así como a cualquier exigencia originada en el principio de responsabilidad demostrada (accountability). Brindar la debida protección a los intereses y necesidades de los titulares de la Información personal tratada por **Givaudan Colombia S.A.S.**

4. Destinatarios

Esta política se aplicará a todas las bases de datos tanto físicas como digitales, que contengan datos personales y que sean objeto de Tratamiento por parte de **Givaudan Colombia S.A.S.**, considerada como responsable. Igualmente, en aquellos casos en que operen como encargadas del tratamiento de datos personales.

La política está dirigida a que la ciudadanía en general tenga a su disposición la información necesaria y suficiente sobre los diferentes tratamientos y fines sobre los que serán objeto sus datos, así como los derechos que ellos, como titulares de datos personales, pueden ejercer frente a **Givaudan Colombia S.A.S.** cuando esta tenga el rol de responsable del tratamiento de sus datos personales.

Esta política es de obligatorio conocimiento y cumplimiento por todos para todas las personas naturales o jurídicas responsables de la administración de bases de datos personales de **Givaudan Colombia S.A.S.**, en especial los administradores del manejo de bases de datos de la SIC y por aquellos funcionarios y contratistas que reciben, atienden y dan respuesta directa o indirectamente a las peticiones (consultas o reclamo) de información relacionadas con la ley de protección de datos personales.

5. Normatividad aplicable

La política de tratamiento de datos de **Givaudan Colombia S.A.S.**, se desarrolla con base en el siguiente marco jurídico:

- Constitución Política, artículo 15
- Ley 1266 de 2008
- Ley 1581 de 2012

regarding Personal Data Protection, as well as any requirement arising from the principle of accountability. To provide due protection to the interests and needs of the owners of the Personal Information processed by **Givaudan Colombia S.A.S.**

4. Addressees

This policy shall apply to all databases, both physical and digital, containing personal data and which are subject to processing by Givaudan Colombia S.A.S., considered responsible. Likewise, in those cases in which they operate as responsible for the processing of personal data.

The policy is aimed at providing citizens in general with the necessary and sufficient information on the different treatments and purposes for which their data will be processed, as well as the rights that they, as holders of personal data, may exercise against **Givaudan Colombia S.A.S.** when it has the role of responsible for the processing of their personal data.

This policy is mandatory knowledge and compliance by all natural or legal persons responsible for the administration of personal data bases of **Givaudan Colombia S.A.S.**, especially the administrators of database management of the SIC and those officials and contractors who receive, attend and respond directly or indirectly to requests (inquiries or claims) for information related to the law of protection of personal data.

5. Applicable regulations

The data processing policy of **Givaudan Colombia S.A.S.**, is developed based on the following legal framework.

- Political Constitution, Article 15
- Law 1266 of 2008
- Law 1581 of 2012
- Regulatory Decree 1727 of 2009
- Regulatory Decree 2952 of 2010
- Partial Regulatory Decree No. 1377 of 2013
- Sole Regulatory Decree 1074 of 2015.

- Decreto Reglamentario 1727 de 2009
- Decreto Reglamentario 2952 de 2010
- Decreto Reglamentario parcial No 1377 de 2013
- Decreto Único Reglamentario 1074 de 2015
- Circular Externa No. 02-2015. Superintendencia de Industria y Comercio.
- Sentencias de la Corte Constitucional C -1011 de 2008 y C - 748 del 2011-

6. Definiciones

Para la correcta interpretación, aplicación y entendimiento esta Política de Procedimientos para el Manejo de Datos, se establecen las definiciones que más adelante se enuncian, las cuales buscan dar un sentido natural a los términos en ellas contenidos, sin excluir la interpretación gramatical de los mismos.

Las definiciones dadas no son taxativas, y en todo caso deberían interpretarse en un sentido lógico y natural conforme a la estructura gramatical donde se estén empleando.

6.1. Autorización: Consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de Datos personales.

6.2. Aviso de privacidad: Comunicación verbal o escrita generada por el Responsable, dirigida al Titular para el Tratamiento de sus datos personales, mediante la cual se le informa acerca de la existencia de las políticas de Tratamiento de información que le serán aplicables, la forma de acceder a las mismas y las finalidades de Tratamiento que se pretende dar a los datos personales.

6.3. Bases de Datos: Conjunto organizado de datos personales que sea objeto de Tratamiento.

6.4. Causahabientes de los datos: persona que ha sucedido a otra por causa del fallecimiento de ésta (heredero).

- External Circular No. 02-2015. Superintendencia of Industry and Commerce.
- Constitutional Court Rulings C -1011 of 2008 and C - 748 of 2011-.

6. Definitions

The following definitions are established for the correct interpretation, application and understanding of this Data Handling Procedures Policy, in order to give a natural meaning to the terms contained therein, without excluding the grammatical interpretation of the same.

The definitions given are not exhaustive, and they should be interpreted in a logical and natural sense according to the grammatical structure where they are being used.

6.1. Authorization: Prior, express and informed consent of the holder to carry out the processing of personal data.

6.2. Privacy Notice: Verbal or written communication generated by the Controller, addressed to the Data Holder for the Processing of his personal data, by means of which he is informed about the existence of the information processing policies that will be applicable, the way to access them and the purposes for which the personal data will be processed.

6.3. Database: Organized set of personal data that is the object of Processing.

6.4. Data heirs: person who has succeeded another person due to the death of the latter (heir).

6.5. Personal data: Any information linked or that can be associated to one or several determined or determinable natural persons. This data may be of a public, semi-private and/or private nature.

6.6. Public data: Data that is not semi-private, private or sensitive. Public data includes, among others, data relating to the civil status of

6.5. Dato Personal o Datos Personales: Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables.

6.6. Dato Público: Es el dato que no sea semiprivado, privado o sensible. Son considerados Datos públicos, entre otros, los Datos relativos al estado civil de las personas, a su profesión u oficio y a su calidad de comerciante o de servidor público. Por su naturaleza, los Datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales y sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva.

6.7. Dato semiprivado: Es semiprivado el dato que no tiene naturaleza íntima, reservada, ni pública y cuyo conocimiento o divulgación puede interesar no sólo a su titular sino a cierto sector o grupo de personas o a la sociedad en general, como el dato financiero y crediticio de actividad comercial o de servicios.

6.8. Dato privado. Es el dato que por su naturaleza íntima o reservada sólo es relevante para el titular.

6.9. Datos Sensibles: Se entiende por Datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los Datos relativos a la salud, a la vida sexual, y los Datos biométricos.

6.10. Datos Biométricos: Son aquellos rasgos físicos, biológicos o de comportamiento de un individuo

individuals, their profession or trade, and their status as merchants or public servants. By their nature, public data may be contained, among others, in public records, public documents, official gazettes and bulletins and duly executed court judgments that are not subject to confidentiality.

6.7. Semi-private data: Semi-private data is data that is not of an intimate, reserved or public nature and whose knowledge or disclosure may be of interest not only to its owner but also to a certain sector or group of persons or to society in general, such as financial and credit data of commercial or service activity.

6.8. Private data. It is data that, due to its intimate or reserved nature, is only relevant to the owner.

6.9. Sensitive data: Sensitive data is understood as that which affects the privacy of the Data Subject or whose improper use may generate discrimination, such as that which reveals racial or ethnic origin, political orientation, religious or philosophical convictions, membership in trade unions, social organizations, human rights organizations or that promotes the interests of any political party or that guarantees the rights and guarantees of opposition political parties, as well as data related to health, sexual life, and biometric data.

6.10. Biometric Data: Those physical, biological or behavioral traits of an individual that identify him/her as unique from the rest of the population, such as fingerprints, DNA analysis.

6.11. Data Processor: " Givaudan", and/or the third party it designates for such function to Francisco Alarcón, id number 79,302.983 through minutes No. 40 of the Extraordinary Shareholders' Meeting of November 7, 2023.

que lo identifican como único del resto de la población como Huellas dactilares, Análisis del ADN.

6.11. Encargado del Tratamiento: Es "Givaudan", y/o el tercero que éste designe para tal función.

6.12. Manual de Políticas y Procedimientos para el Manejo de Datos Personales: Son las directrices y procedimientos adoptados por "Givaudan", para la recolección y tratamiento de Datos Personales (en adelante Manual).

6.13. Responsable del Tratamiento: Será el Oficial de Privacidad que ha sido designado por "Givaudan", Francisco Alarcón, mayor de edad, identificado con la cédula de ciudadanía No. 79,302.983, mediante acta No 40 de Asamblea Extraordinaria de Accionistas del 7 de noviembre de 2023.

6.14. Política de Tratamiento: Se refiere al presente documento, como política de tratamiento de datos personales aplicada por La Empresa de conformidad con los lineamientos de la legislación vigente en la materia.

6.15. Titular: Es la persona natural o jurídica a quien se refiere la información que reposa en un banco de datos. Esta persona es sujeto del derecho de hábeas data.

6.16. Tratamiento: Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión de Datos Personales.

6.17. Transferencia: La transferencia de datos tiene lugar cuando el responsable y/o Encargado del Tratamiento de Datos Personales, ubicado en Colombia, envía la información o los Datos Personales a un receptor, que a su vez es responsable

6.12. Policies and Procedures Manual for the Handling of Personal Data: These are the guidelines and procedures adopted by "Givaudan" for the collection and processing of Personal Data (hereinafter Manual).

6.13. Data Controller: The Privacy Officer who has been appointed by "Givaudan", Francisco Alarcón, of legal age, identified with citizenship card 79,302,983, by means of act No. 40 of the Extraordinary Shareholders' Meeting of November 7, 2023.

6.14. Processing Policy: Refers to this document, as the personal data processing policy applied by The Company in accordance with the guidelines of the legislation in force on the matter.

6.15. Owner of the information. It is the natural or legal person to whom the information contained in a database refers. This person is subject to the right of habeas data.

6.16. Processing: Any operation or set of operations on personal data, such as the collection, storage, use, circulation or deletion of Personal Data.

6.17. Transfer: The transfer of data takes place when the Controller and/or Processor of personal data, located in Colombia, sends the information or personal data to a recipient, which in turn is the Data Controller and is located inside or outside the country.

6.18. Transmission: Processing of personal data that involves the communication of such data within or outside the territory of the Republic of Colombia when its purpose is the

del Tratamiento y se encuentra dentro o fuera del país.

6.18. Transmisión: Tratamiento de Datos Personales que implica la comunicación de los mismos dentro o fuera del territorio de la República de Colombia cuando tenga por objeto la realización de un Tratamiento por el Encargado por cuenta del responsable.

6.19. Recepción PQRS - tratamiento de datos: Toda solicitud del titular del dato para corregir, actualizar, suprimir sus datos personales o para revocar la autorización en los casos establecidos en la ley, ya sean recibidas a través de correo electrónico, telefónicamente, personalmente y/o direccionadas desde otros procesos internos de Givaudan Colombia S.A.S. se direccionarán así: francisco.alarcon@givaudan.com. Responsable: **Francisco Alarcón** Oficial de Privacidad (“OP”) designado por Givaudan.

6.20. Verificación y registro: Si la solicitud está completa, debe consultar a los responsables de las bases de datos, y estos a su vez deben tramitar la solicitud y responder al proceso de servicio al Titular de la información personal, quienes deben contactarse en un plazo no mayor a 2 días hábiles a través de correo electrónico, telefónicamente y/o correspondencia con el titular; e indicarle el estado de la solicitud “reclamo en trámite” además de registrar en la base de datos la observación, e ingresar la causa en la siguiente clasificación: conocer los datos almacenados y el uso de los mismos, actualizar datos personales, rectificar los datos almacenados, revocar la autorización para el tratamiento de datos, suprimir los datos almacenados y/o derecho vulnerado. La leyenda se mantendrá hasta que el reclamo sea decidido.

6.21. Direccionamiento: Una vez determinada la respuesta a la solicitud, se debe informar a los responsables de

performance of a Processing by the Processor on behalf of the Controller.

6.19. PQRS reception - data processing: All requests from the data holder to correct, update, delete their personal data or to revoke the authorization in the cases established by law, whether received via email, telephone, in person and/or directed from other internal processes of Givaudan Colombia S.A.S. will be addressed as follows: francisco.alarcon@givaudan.com Person Controller Francisco Alarcón Privacy Officer (“PO”) designated by Givaudan. (“PO”).

6.20. Verification and registration: If the request is complete, you must consult the responsible for the databases, and these in turn must process the request and respond to the process of service to the holder of personal information, who must be contacted within a period not exceeding 2 working days via email, telephone and / or correspondence with the holder; and indicate the status of the request "claim in process" in addition to registering in the database the observation, and enter the cause in the following classification: know the stored data and the use of the same, update personal data, rectify the stored data, revoke the authorization for data processing, delete the stored data and / or violated right. The legend will be maintained until the claim is decided.

6.21. Addressing: Once the response to the request has been determined, the persons controller for the databases must be informed so that they may proceed with the appropriate attention to the claim within the frame established in section 15 of this policy. Person Controller Francisco Alarcón Privacy

las bases de datos para que procedan en torno a la atención idónea del reclamo en el tiempo establecido en el numeral 15 de la presente política. Responsable: Francisco Alarcón Oficial de Privacidad (“OP”) designado por Givaudan.

6.22. Actuación requerida: Realizar la modificación, supresión y/o rectificación de los datos, e informar al proceso de Servicio al Titular de la información personal en un plazo no mayor a dos (2) días hábiles.

6.23. Concepto Jurídico: Si la causa del PQR es la causa “DERECHO VULNERADO”, se debe direccionar al área jurídica, para su tratamiento, revisión, solución y respuesta.

6.24. Notificación: Notificar al titular de la solución de su PQR a través del canal elegido por el titular. RESPONSABLE Oficial de Privacidad (“OP”).

6.25. Requerimientos: Solicitud por parte del Titular de la información personal ante “GIVAUDAN” por alguna inconformidad respecto del tratamiento de su información personal los cuales están divididos en:

6.26. Reclamo: Manifestación verbal o escrita de insatisfacción del Titular de la información personal, puesta en conocimiento de “GIVAUDAN”, sobre el tratamiento de información personal que requiera un trámite interno por parte de “GIVAUDAN”.

6.27. Queja: Manifestación verbal o escrita de inconformidad del Titular de la información personal, asociada a la forma y condiciones en que se ha dado tratamiento de la información personal bien sea porque la misma se ha tratado por parte de Givaudan en condiciones distintas a las finalidades autorizadas, o porque no se ha contado con la autorización previa y expresa que determina el ordenamiento jurídico colombiano.

Officer (“PO”) designated by Givaudan. (“PO”).

6.22. Required action: Make the modification, deletion and/or rectification of the data, and inform the process of Service to the Holder of the personal information within a period not exceeding two (2) business days.

6.23. Legal Concept: If the cause of the PQR is “RIGHT VULNERATED”, it should be directed to the legal area for treatment, review, solution and response.

6.24. Notification: Notify the holder of the solution of his/her PQR through the channel chosen by the holder. RESPONSIBLE Privacy Officer (“PO”).

6.25. Requests: Request by the Holder of personal information to “GIVAUDAN ” for any disagreement regarding the processing of personal information which are divided into:

6.26. Claim: Verbal or written manifestation of dissatisfaction of the Holder of the personal information, brought to the attention of “GIVAUDAN ”, regarding the processing of personal information that requires an internal procedure by “GIVAUDAN ”.

6.27. Complaint: Verbal or written statement of disagreement of the Holder of the personal information, associated with the form and conditions in which the personal information has been treated, either because it has been treated by Givaudan in conditions different from the authorized purposes, or because it has not had the prior and express authorization determined by the Colombian legal system.

6.28. Petición: Se trata de cualquier solicitud de información asociada al tratamiento de la información personal cuyo responsable es "GIVAUDAN " ó cualquier manifestación verbal o escrita del Titular de la información personal, mediante la cual solicite ante la empresa algún derecho derivado del uso de su información personal en atención a lo dispuesto en el ordenamiento jurídico colombiano.

6.29. Solicitud: Comunicación verbal o escrita puesta en conocimiento de "GIVAUDAN", en la búsqueda de obtener acceso a la información sobre temas relacionados con el tratamiento de su información personal.

6.30. Sugerencia: Es una recomendación verbal o escrita que presenta el Titular de la información personal para mejorar un proceso cuyo objeto está relacionado con el manejo de la información personal.

6.31. PQR: Peticiones, quejas, reclamos, solicitudes y sugerencias.

6.32. SNG: sistema de gestión web que contiene la aplicación Gestión de Reclamos.

6.33. "OP": Hace referencia al oficial de Privacidad de Givaudan.

7. Principios rectores

El presente Manual de Políticas de Tratamiento de la Información que **La Empresa** posee, se regirá por los siguientes principios:

- **Principio de Legalidad:** El Tratamiento de los datos personales es una actividad reglada que debe sujetarse a lo

6.28. Petition: This is any request for information associated with the processing of personal information for which "GIVAUDAN " is responsible, or any verbal or written statement by the Holder of the personal information, by which he/she requests the company any right derived from the use of his/her personal information in accordance with the provisions of the Colombian legal system.

6.29. Request: Verbal or written communication brought to the attention of "GIVAUDAN ", seeking to obtain access to information on issues related to the processing of your personal information.

6.30. Suggestion: It is a verbal or written recommendation submitted by the Holder of personal information to improve a process whose object is related to the handling of personal information.

6.31. PQR: Petitions, complaints, claims, requests and suggestions.

6.32. SNG: web management system containing the Claims Management application.

6.33. "OP": refers to the Givaudan Privacy Officer.

7. Guiding Principles

The present Manual of Policies of Treatment of the Information that **The Company** possesses, will be governed by the following principles:

- **Principle of legality:** The processing referred to in this policy must be subject to the provisions of this policy and other provisions that develop it.

establecido en la Ley 1581 de 2012 y en las demás disposiciones que las desarrollen.

- **Principio de Finalidad:** El Tratamiento de los datos personales debe obedecer a una finalidad legítima de acuerdo con la Constitución y la Ley, la cual debe ser informada al Titular.

- **Principio de Libertad:** El Tratamiento de los datos personales sólo puede ejercerse con el consentimiento, previo, expreso e informado del Titular. Los datos personales no podrán ser obtenidos o divulgados sin previa autorización, o en ausencia de mandato legal o judicial que releve el consentimiento.

- **Principio de Veracidad o Calidad:** La información contenida en las bases de datos debe ser veraz, completa, exacta, actualizada, comprobable y comprensible. Se prohíbe el Tratamiento de datos parciales, incompletos, fraccionados o que induzcan a error.

- **Principio de Transparencia:** En el Tratamiento debe garantizarse el derecho del Titular a obtener del Responsable o Encargado del Tratamiento, en cualquier momento y sin restricciones, información acerca de la existencia de datos que le conciernan.

- **Principio de Acceso y Circulación Restringida:** El Tratamiento se sujeta a los límites que se derivan de la naturaleza de los datos personales, de las disposiciones de la ley y la Constitución. En este sentido, el Tratamiento sólo podrá hacerse por personas autorizadas por el Titular y/o por las personas previstas en la ley. Los datos personales, salvo la información pública, no podrán estar disponibles en Internet u otros medios de divulgación o comunicación masiva, salvo que el acceso sea técnicamente controlable para brindar un conocimiento restringido sólo a los Titulares o terceros autorizados conforme a la ley.

- **Principle of purpose.** The processing must obey a legitimate purpose in accordance with the constitution and the law, which must be informed to the owner.

- **Principle of Freedom:** The processing of personal data can only be exercised with the prior, express and informed consent of the Data Subject. Personal data may not be obtained or disclosed without prior authorization, or in the absence of legal or judicial mandate that relieves the consent.

- **Principle of truthfulness or quality.** The information contained in the databases must be truthful, complete, accurate, updated, verifiable and understandable. The recording and disclosure of partial, incomplete, fractioned or misleading data is prohibited.

- **Principle of transparency.** The right of the Data Subject to obtain from The Company or the Data Processor, at any time and without restrictions, information about the existence of data concerning him/her, must be guaranteed in the Processing.

- **Principle of restricted access and circulation.** The Processing is subject to the limits derived from the nature of the personal data, the provisions of the law and the Constitution. In this sense, the Processing may only be carried out by persons authorized by the Holder and/or by the persons provided for by law. Personal data, except for public information, may not be available on the Internet or other means of dissemination or mass communication, unless access is technically controllable to provide restricted knowledge only to the Holders or third parties authorized by law.

- **Principle of temporality of the information.** The holder's information may not be provided to users or

• **Principio de Temporalidad de la información:** agotada la finalidad para la cual fue recolectado y/o tratado el dato personal, el responsable o encargado cesará su uso.

• **Principio de Seguridad:** La información sujeta a Tratamiento por el Responsable o Encargado del Tratamiento, se deberá manejar con las medidas técnicas, humanas y administrativas que sean necesarias para otorgar seguridad a los registros evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.

• **Principio de Confidencialidad:** Todas las personas que intervengan en el Tratamiento de datos personales que no tengan la naturaleza de públicos están obligadas a garantizar la reserva de la información, inclusive después de finalizada su relación con alguna de las labores que comprende el Tratamiento, pudiendo sólo realizar suministro o comunicación de datos personales cuando ello corresponda al desarrollo de las actividades autorizadas en la ley y en los términos de la misma.

• **Interpretación integral de los derechos constitucionales:** Los derechos se interpretarán en armonía y en un plano de equilibrio con el derecho a la información previsto en el artículo 20 de la Constitución y con los derechos constitucionales aplicables.

• **Principio de Necesidad:** Los datos personales tratados deben ser los estrictamente necesarios para el cumplimiento de las finalidades perseguidas con la base de datos.

8. Tipología de los Datos

8.1. Datos sensibles.

Conforme a lo establecido en el acápite de Definiciones, son Datos Sensibles *aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de*

third parties when it ceases to serve the purpose of the database.

• **Security Principle:** The information subject to processing by the Company or the Data Processor shall be handled with the technical, human and administrative measures necessary to provide security to the records avoiding their adulteration, loss, consultation, use or unauthorized or fraudulent access.

• **Principle of confidentiality.** All persons involved in the processing of personal data that are not of a public nature are obliged to guarantee the confidentiality of the information, even after the end of their relationship with any of the tasks involved in the processing, and may only provide or communicate personal data when it corresponds to the development of the activities authorized in the regulations in force.

• **Integral interpretation of constitutional rights:** The rights shall be interpreted in harmony and in balance with the right to information provided for in Article 20 of the Constitution and with the applicable constitutional rights.

• **Principle of Necessity:** The personal data processed must be strictly necessary for the fulfillment of the purposes pursued with the database.

8. Data Typology

8.1. Sensitive Data.

As established in the Definitions section, Sensitive Data are those that affect the privacy of the Data Subject or whose improper use may generate discrimination, such as those that reveal racial or ethnic origin, political orientation, religious or philosophical

derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición así como los datos relativos a la salud, a la vida sexual y los datos biométricos.

La Empresa solamente podrá dar tratamiento a este tipo de datos, en los siguientes casos:

- 8.1.1. El Titular haya dado su autorización explícita a dicho Tratamiento, salvo en los casos que por ley no sea requerido el otorgamiento de dicha autorización;
- 8.1.2. El Tratamiento sea necesario para salvaguardar el interés vital del Titular y este se encuentre física o jurídicamente incapacitado. En estos eventos, los representantes legales deberán otorgar su autorización;
- 8.1.3. El Tratamiento sea efectuado en el curso de las actividades legítimas y con las debidas garantías por parte de una fundación, ONG, asociación o cualquier otro organismo sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, siempre que se refieran exclusivamente a sus miembros o a las personas que mantengan contactos regulares por razón de su finalidad. En estos eventos, los datos no se podrán suministrar a terceros sin la autorización del Titular;
- 8.1.4. El Tratamiento se refiera a datos que sean necesarios para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial;
- 8.1.5. El Tratamiento tenga una finalidad histórica, estadística o científica. En este evento deberán adoptarse las medidas conducentes a la supresión de identidad de los Titulares.

En todo caso, y dada la naturaleza de este tipo de datos, **La Empresa** debe sujetarse al cumplimiento de las siguientes obligaciones:

- 8.1.6. Informar al Titular que por tratarse de datos sensibles no está obligado a autorizar su Tratamiento.
- 8.1.7. Informar al Titular de forma explícita y previa, además de los requisitos generales de la autorización para la

convicciones, membership in unions, social organizations, human rights organizations or that promote the interests of any political party or that guarantee the rights and guarantees of opposition political parties, as well as data related to health, sex life and biometric data.

The Company may only process this type of data in the following cases:

- 8.1.1. The Data Subject has given his/her explicit authorization to such Processing, except in those cases where by law the granting of such authorization is not required;
- 8.1.2. The Processing is necessary to safeguard the vital interest of the Data Subject and he/she is physically or legally incapacitated. In these events, the legal representatives must grant their authorization;
- 8.1.3. The Processing is carried out in the course of legitimate activities and with due guarantees by a foundation, NGO, association or any other non-profit organization, whose purpose is political, philosophical, religious or trade union, provided that it refers exclusively to its members or to persons who maintain regular contacts due to its purpose. In these events, the data may not be provided to third parties without the authorization of the Data Controller;
- 8.1.4. The Processing refers to data that are necessary for the recognition, exercise or defense of a right in a legal proceeding;
- 8.1.5. The Processing has a historical, statistical or scientific purpose. In this event, the measures leading to the suppression of the identity of the Data Holders must be adopted.

recolección de cualquier tipo de dato personal, cuáles de los datos que serán objeto de Tratamiento son sensibles y la finalidad del Tratamiento, así como obtener su consentimiento expreso.

8.2.Datos Públicos

De acuerdo a lo establecido en el acápite de definiciones, son datos públicos aquellos *que no sean semiprivados, privados o sensibles. Son considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio y a su calidad de comerciante o de servidor público. Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales y sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva.*

Siempre que se trate de datos de esta naturaleza, **La Empresa** podrá realizar el tratamiento de los mismos, conforme a las prescripciones legales vigentes.

8.3.Datos Semiprivados y Datos Privados

Para el tratamiento de este tipo de datos, **La Empresa** deberá contar con la correspondiente autorización del titular de la información, dada su naturaleza. Esta autorización se realizará con base a lo establecido en la Constitución y la normativa vigente, así como a lo determinado en el numeral 5.4 de este Manual de Políticas de Tratamiento de la Información.

8.4.Autorización del Titular

Sin perjuicio de las excepciones previstas en la ley, en el Tratamiento se requiere la autorización previa e informada del Titular, la cual deberá ser obtenida por cualquier medio que pueda ser objeto de consulta y verificación posterior.

In any case, and given the nature of this type of data, **The Company** must comply with the following obligations:

8.1.6. Inform the Data Subject that, since the data is sensitive, he/she is not obliged to authorize its Processing.

8.1.7. Inform the Data Subject explicitly and in advance, in addition to the general requirements for authorization for the collection of any type of personal data, which of the data to be processed are sensitive and the purpose of the Processing, as well as obtain their express consent.

8.2. Public Data

As established in the definitions section, public data are those that are not semi-private, private or sensitive. Public data includes, among others, data related to the marital status of individuals, their profession or trade, and their status as merchants or public servants. By their nature, public data may be contained, among others, in public records, public documents, official gazettes and bulletins, and duly executed court rulings that are not subject to confidentiality.

Whenever data of this nature are involved, **the Company** may process them in accordance with the legal requirements in force.

8.3. Semi-Private Data and Private Data

For the processing of this type of data, **The Company** must have the corresponding authorization from the owner of the information, given its nature. This authorization shall be made based on the provisions of the Constitution and current regulations, as well as the provisions of section 5.4 of this Information Processing Policy Manual.

8.4.1. Casos en los cuales no se requiere de la autorización del Titular:

- 8.4.1.1. Información requerida por una entidad pública o administrativa en ejercicio de sus funciones legales o por orden judicial;
- 8.4.1.2. Datos de naturaleza pública;
- 8.4.1.3. Casos de urgencia médica o sanitaria;
- 8.4.1.4. Tratamiento de información autorizado por la ley para fines históricos, estadísticos o científicos;
- 8.4.1.5. Datos relacionados con el Registro Civil de las Personas.

9. Derechos de los niños, niñas y adolescentes

En el tratamiento de los datos de los derechos de los niños, niñas y adolescentes, cuando este esté permitido, **La Empresa** deberá cumplir los siguientes requisitos y deberá sujetarse a los siguientes parámetros:

- 9.1. Que el tratamiento responda y respete el interés superior de los niños, niñas y adolescentes
- 9.2. Que en el tratamiento se asegure el respeto de sus derechos fundamentales
- 9.3. **La Empresa** deberá contar con la autorización del representante legal del menor.
- 9.4. **La Empresa** deberá escuchar al menor, respetando en todo caso su opinión, la cual deberá ser valorada teniendo en cuenta su madurez, autonomía y capacidad para entender el asunto.

Ahora bien, a efectos que El Titular pueda conocer en qué casos es posible realizar un tratamiento respecto de los datos de los niños, niñas y adolescentes, dichos casos son los siguientes:

- 9.5. Los datos de naturaleza pública, los cuales se encuentran definidos en el acápite de definiciones de este Manual.

8.4. Authorization of the Data Owner

Notwithstanding the exceptions provided by law, the processing requires the prior and informed authorization of the Data Subject, which must be obtained by any means that may be subject to consultation and subsequent verification.

8.4.1. Cases in which the authorization of the Data Holder is not required:

- 8.4.1.1. Information required by a public or administrative entity in exercise of its legal functions or by court order;
- 8.4.1.2. Data of a public nature;
- 8.4.1.3. Cases of medical or sanitary urgency;
- 8.4.1.4. Processing of information authorized by law for historical, statistical or scientific purposes;
- 8.4.1.5. Data related to the Civil Registry of Persons.

9. Rights of children and adolescents

In the processing of data on the rights of children and adolescents, when permitted, **The Company** shall comply with the following requirements and shall be subject to the following parameters:

- 9.1. That the treatment responds to and respects the best interests of children and adolescents.
- 9.2. That the treatment ensures respect for their fundamental rights.
- 9.3. The Company shall have the authorization of the legal representative of the minor.
- 9.4. **The Company** shall listen to the minor, respecting in any case his or her opinion, which shall be assessed taking into account his or her maturity, autonomy and capacity to understand the matter.

10. Deberes de la Empresa como responsable y encargado del tratamiento

Siempre que La Empresa, como responsable del tratamiento de los datos de El Titular, tenga información que pueda ser objeto de modificación, verificación, rectificación, consulta y/o eliminación, deberá:

- a.** Garantizar al Titular, en todo tiempo, el pleno y efectivo ejercicio del derecho de hábeas data;
- b.** Solicitar y conservar, en las condiciones previstas en la ley, copia de la respectiva autorización otorgada por el Titular;
- c.** Informar debidamente al Titular sobre la finalidad de la recolección y los derechos que le asisten por virtud de la autorización otorgada;
- d.** Conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento;
- e.** Garantizar que la información que se suministre al Encargado del Tratamiento sea veraz, completa, exacta, actualizada, comprobable y comprensible;
- f.** Actualizar la información, comunicando de forma oportuna al Encargado del Tratamiento, todas las novedades respecto de los datos que previamente le haya suministrado y adoptar las demás medidas necesarias para que la información suministrada a este se mantenga actualizada;
- g.** Rectificar la información cuando sea incorrecta y comunicar lo pertinente al Encargado del Tratamiento;
- h.** Suministrar al Encargado del Tratamiento, según el caso, únicamente datos cuyo Tratamiento esté previamente autorizado de conformidad con lo previsto en la ley.

Now, in order for the Data Holder to be able to know in which cases it is possible to process the data of children and adolescents, such cases are the following:

- 9.5. Data of a public nature, which are defined in the definitions section of this Manual.

10. Duties of the Company as Data Controller and Data Processor

Whenever The Company, as data controller of The Data Subject, has information that may be subject to modification, verification, rectification, consultation and/or deletion, it shall:

- a.** Guarantee the Data Subject, at all times, the full and effective exercise of the right of habeas data;
- b.** Request and keep, under the conditions provided by law, a copy of the respective authorization granted by the Data Subject;
- c.** Duly inform the Data Subject about the purpose of the collection and the rights he/she has by virtue of the authorization granted;
- d.** Keep the information under the necessary security conditions to prevent its adulteration, loss, consultation, use or unauthorized or fraudulent access;
- e.** Guarantee that the information provided to the Data Processor is truthful, complete, accurate, updated, verifiable and understandable;
- f.** Update the information, communicating in a timely manner to the Data Processor, all developments with respect to the data previously provided and take other necessary measures to ensure that the information provided to it is kept up to date;

i. Exigir al Encargado del Tratamiento en todo momento, el respeto a las condiciones de seguridad y privacidad de la información del Titular;

j. Tramitar las consultas y reclamos formulados por el Titular de la información, en los términos señalados en la ley;

k. Adoptar un manual interno de políticas y procedimientos para garantizar el adecuado cumplimiento de la ley y en especial, para la atención de consultas y reclamos;

l. Informar al Encargado del Tratamiento cuando determinada información se encuentra en discusión por parte del Titular, una vez se haya presentado la reclamación y no haya finalizado el trámite respectivo;

m. Informar a solicitud del Titular sobre el uso dado a sus datos;

n. Informar a la autoridad de protección de datos cuando se presenten violaciones a los códigos de seguridad y existan riesgos en la administración de la información de los Titulares;

o. Cumplir las instrucciones y requerimientos que imparta la Superintendencia de Industria y Comercio;

p. Informar a El Titular, los cambios, adiciones y/o modificaciones a estas políticas de uso de la información que consten en sus bases de datos.

g. Rectify the information when it is incorrect and communicate the pertinent to the Data Processor;

h. To provide to the Data Processor, as the case may be, only data whose Processing is previously authorized in accordance with the provisions of the law.

i. To demand from the Data Processor, at all times, respect for the security and privacy conditions of the Data Subject's information;

j. To process the queries and claims formulated by the Data Subject, under the terms set forth in the law;

k. Adopt an internal manual of policies and procedures to ensure proper compliance with the law and, in particular, for the handling of queries and claims;

l. Inform the Data Processor when certain information is under discussion by the Data Subject, once the claim has been filed and the respective process has not been completed;

m. To inform, at the request of the Data Subject, about the use given to his/her data;

n. Inform the data protection authority when there are violations to the security codes and there are risks in the administration of the information of the Data Controllers;

o. Comply with the instructions and requirements given by the Superintendence of Industry and Commerce;

p. Inform the Holder of any changes, additions and/or modifications to these policies of use of the information contained in its databases.

La Empresa cumplirá los siguientes deberes como Encargado del Tratamiento de los Datos Personales del Titular:

- a.** Garantizar al Titular, en todo tiempo, el pleno y efectivo ejercicio del derecho de hábeas data;
- b.** Conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento;
- c.** Realizar oportunamente la actualización, rectificación o supresión de los datos;
- d.** Actualizar la información reportada por los Responsables del Tratamiento dentro de los cinco (5) días hábiles contados a partir de su recibo;
- e.** Tramitar las consultas y los reclamos formulados por los Titulares en los términos señalados en la ley y en este Manual;
- f.** Adoptar un manual interno de políticas y procedimientos para garantizar el adecuado cumplimiento de la ley y, en especial, para la atención de consultas y reclamos por parte de los Titulares;
- g.** Registrar en la base de datos la leyenda “reclamo en trámite” en la forma en que se regula en la ley;
- h.** Insertar en la base de datos la leyenda “información en discusión judicial” una vez notificado por parte de la autoridad competente sobre procesos judiciales relacionados con la calidad del dato personal;
- i.** Abstenerse de circular información que esté siendo controvertida por el Titular y cuyo bloqueo haya sido ordenado por la Superintendencia de Industria y Comercio;
- j.** Permitir el acceso a la información únicamente a las personas que pueden tener acceso a ella;
- k.** Informar a la Superintendencia de Industria y Comercio cuando se presenten violaciones a los códigos de seguridad y

The Company shall comply with the following duties as Data Controller of the Personal Data of the Data Subject:

- a.** Guarantee the Data Subject, at all times, the full and effective exercise of the right of habeas data;
- b.** Keep the information under the security conditions necessary to prevent its adulteration, loss, consultation, unauthorized or fraudulent use or access;
- c.** To update, rectify or delete data in a timely manner;
- d.** Update the information reported by the Data Controllers within five (5) business days from its receipt;
- e.** To process the queries and claims made by the Data Controllers under the terms set forth in the law and in this Manual;
- f.** Adopt an internal manual of policies and procedures to ensure proper compliance with the law and, in particular, for the attention of queries and claims by the Holders;
- g.** Register in the database the legend "claim in process" in the manner regulated by law;
- h.** Insert in the database the legend "information under judicial discussion" once notified by the competent authority about judicial proceedings related to the quality of the personal data;
- i.** Refrain from circulating information that is being disputed by the Data Subject and whose blocking has been ordered by the Superintendence of Industry and Commerce;
- j.** To allow access to the information only to the persons who may have access to it; j. To allow access to the information only to the persons who may have access to it;

existan riesgos en la administración de la información de los Titulares;

I. Cumplir las instrucciones y requerimientos que imparta la Superintendencia de Industria y Comercio.

11. Finalidades

La Empresa como entidad respetuosa de la privacidad de las personas reconoce que el Titular de los datos personales tiene derecho a contar con elementos adecuados que garanticen la misma, teniendo en todo caso para ello en cuenta sus responsabilidades, derechos y obligaciones.

En virtud de la relación que se ha establecido o se establezca entre el Titular de los datos personales y **La Empresa**, es importante que este conozca que **La Empresa** recolecta, registra, almacena, usa los datos personales de los Titulares, para su propio uso con los propósitos que fueron solicitados o por requerimientos de las entidades públicas.

Los Datos Personales de los Titulares son utilizados por **La Empresa** para:

11.1. Ejecutar las actividades propias de **La Empresa** para cumplir su objeto social, todo lo cual se hará con base en la finalidad de la Base de Datos en la que reposan los Datos Personales de los Titulares.

11.2. Ofrecerle los productos, servicios y o beneficios que buscan satisfacer las necesidades de los Titulares, o los productos y servicios de **La Empresa**, lo cual puede hacerse por medios físicos o a través de correos electrónicos y/o terminales móviles.

11.3. Enviar la información a entidades gubernamentales por exigencia legal.

k. Inform the Superintendence of Industry and Commerce when there are violations to the security codes and there are risks in the administration of the information of the Holders;

I. Comply with the instructions and requirements given by the Superintendence of Industry and Commerce.

11. Purposes

The Company, as an entity respectful of the privacy of individuals, recognizes that the Owner of the personal data has the right to have adequate elements to ensure the same, taking into account their responsibilities, rights and obligations.

By virtue of the relationship that has been or will be established between the Holder of the personal data and **The Company**, it is important that the latter knows that **The Company** collects, registers, stores, uses the personal data of the Holders, for its own use for the purposes that were requested or by requirements of public entities.

The Personal Data of the Data Controllers are used by **The Company** for:

11.1. Execute the activities of The Company to fulfill its corporate purpose, all of which will be done based on the purpose of the Database in which the Personal Data of the Data Controllers are stored.

11.2. To offer the products, services and/or benefits that seek to satisfy the needs of the Data Subjects, or the products and services of The Company, which may be done by physical means or through e-mails and/or mobile terminals.

11.3. To send the information to governmental entities as required by law.

11.4. Consultar información en las listas de control (Listas Nacionales e Internacionales), consultar a la CIFI, a las centrales de información, Lista Clinton, Procuraduría, Contraloría, Policía Nacional, DIJIN con el fin de preservar la confianza y transparencia entre el Titular de los Datos y **La Empresa**.

11.5. Soportar procesos de auditoría externa e interna.

11.6. Para la ejecución de procesos de índole judicial y extrajudicial en los casos permitidos por los Estatutos y Reglamentos de **La Empresa**.

11.7. Registrar la información de Empleados, exempleados, proveedores, clientes (activos e inactivos) en las bases de datos de **La Empresa**, para el envío de información contractual, comercial y obligacional a que hubiere lugar.

11.8. Para verificación de referencias de empleados, exempleados, proveedores, clientes (activos e inactivos) en las bases de datos.

11.9. Respecto de la recolección y tratamiento de datos realizados mediante mecanismos automatizados con el objeto de generar registros de actividad de los visitantes y registros de audiencia **La Empresa**, sólo podrá utilizar dicha información para la elaboración de informes que cumplan con los objetivos señalados. En ningún caso podrá realizar operaciones que impliquen asociar dicha información a algún usuario identificado o identificable.

11.10. Efectuar encuestas para evaluar las propuestas de fragancias en el desarrollo de los proyectos del negocio;

11.11. Realizar actividades de publicidad y prospección comercial, así como encuestas de opinión;

11.12. Efectuar las gestiones pertinentes para el desarrollo del objeto social de la compañía en lo que tiene que ver con el cumplimiento del objeto del contrato celebrado con el Titular de la información;

11.4. Consult information in the control lists (National and International Lists), consult the CIFI, information centers, Clinton List, Attorney General's Office, Comptroller's Office, National Police, DIJIN in order to preserve the trust and transparency between the Data Subject and The Company.

11.5. To support external and internal auditing processes.

11.6. For the execution of judicial and extrajudicial processes in the cases allowed by the Bylaws and Regulations of The Company.

11.7. To register the information of Employees, former employees, suppliers, customers (active and inactive) in the Company's databases, for the sending of contractual, commercial and obligatory information as the case may be.

11.8. For verification of references of employees, former employees, suppliers, customers (active and inactive) in the databases.

11.9. Regarding the collection and processing of data through automated mechanisms in order to generate records of visitor activity and audience records, The Company may only use such information for the preparation of reports that meet the stated objectives. Under no circumstances may it carry out operations that imply associating said information to any identified or identifiable user.

11.10. Conduct surveys to evaluate fragrance proposals in the development of business projects;

11.11. To carry out advertising and commercial prospecting activities, as well as opinion polls;

11.12. To carry out the pertinent actions for the development of the company's corporate purpose in relation to the fulfillment of the purpose of the contract entered into with the Data Subject;

<p>11.13. Promoción, selección y gestión de personal;</p> <p>11.14. Ofrecer programas de bienestar corporativo y planificar actividades empresariales, para el titular y sus beneficiarios como: fechas especiales, atención a auditorias, procesos administrativos, entre otros;</p> <p>11.15. Seguridad y control acceso a edificios;</p> <p>11.16. Video vigilancia;</p> <p>11.17. Transmitir los datos personales fuera del país a terceros con los cuales Givaudan Colombia S.A.S. haya suscrito un contrato de procesamiento de datos y sea necesario entregársela para el cumplimiento del objeto contractual;</p> <p>11.18. Contactar al titular a través de correo electrónico para el envío de extractos, estados de cuenta o facturas en relación con las obligaciones derivadas del contrato celebrado entre las partes;</p> <p>11.19. Gestión contable, fiscal y administrativa de proveedores y clientes;</p> <p>11.20. Contactar al titular a través de medios telefónicos para realizar encuestas, estudios y/o confirmación de datos personales necesarios para la ejecución de una relación contractual.</p>	<p>11.13. Promotion, selection and management of personnel;</p> <p>11.14. Offer corporate welfare programs and plan business activities, for the holder and its beneficiaries such as: special dates, attention to audits, administrative processes, among others;</p> <p>11.15. Security and building access control;</p> <p>11.16. Video surveillance;</p> <p>11.17. Transmit personal data outside the country to third parties with whom Givaudan Colombia S.A.S. has entered into a data processing contract and it is necessary to deliver it to them for the fulfillment of the contractual purpose;</p> <p>11.18. Contact the holder via e-mail to send statements, account statements or invoices in connection with the obligations arising from the contract entered into between the parties;</p> <p>11.19. Accounting, fiscal and administrative management of suppliers and customers;</p> <p>11.20. Contacting the holder through telephone means to conduct surveys, studies and/or confirmation of personal data necessary for the execution of a contractual relationship.</p>
<p>12. Derechos de los titulares de la información</p> <p>Los Titulares de la Información que consten en las bases de datos de La Empresa, podrán ejercer en cualquier tiempo los siguientes derechos:</p> <p>a. Conocer, actualizar, cancelar y rectificar sus datos personales frente a los Responsables del Tratamiento o Encargados del Tratamiento. Este derecho se podrá ejercer,</p>	<p>12. Rights of the Data Holders</p> <p>The Owners of the information contained in the Company's databases may exercise the following rights at any time:</p> <p>a. To know, update, cancel and rectify their personal data against the Data Controllers or Data Processors. This right may be exercised, among</p>

entre otros frente a datos parciales, inexactos, incompletos, fraccionados, que induzcan a error, o aquellos cuyo Tratamiento esté expresamente prohibido o no haya sido autorizado.

b. Solicitar prueba de la autorización otorgada al Responsable del Tratamiento salvo cuando expresamente se exceptúe como requisito para el Tratamiento.

c. Ser informado por el Responsable o el Encargado del Tratamiento, previa solicitud, respecto del uso que le ha dado a sus datos personales.

d. Presentar ante la Superintendencia de Industria y Comercio quejas por infracciones a lo dispuesto en la normatividad vigente, siempre que se agote previamente el trámite interno de consulta o reclamación de que trata este Manual de Políticas, el cual, conforme a las prescripciones de ley, es requisito de procedibilidad.

e. Revocar la autorización y/o solicitar la supresión del dato cuando en el Tratamiento no se respeten los principios, derechos y garantías constitucionales y legales.

f. Acceder en forma gratuita a sus datos personales que hayan sido objeto de Tratamiento, en las condiciones señaladas en este Manual de Políticas y la ley.

g. El derecho a que no se le condicione en ningún caso, para el desarrollo de cualquier actividad con La Empresa, que deba estar obligado al suministro de sus datos personales sensibles.

13. Autorización y consentimiento del titular para el tratamiento de datos

Toda la información que La Empresa pueda recopilar, almacenar, circular, utilizar, modificar, rectificar y/o suprimir respecto de los titulares de la misma, deberá contar con el consentimiento expreso, previo, libre e informado del Titular de la Información.

others, against partial, inaccurate, incomplete, fractioned, misleading data, or data whose processing is expressly prohibited or has not been authorized.

b. Request proof of the authorization granted to the Data Controller, except when expressly exempted as a requirement for the Processing.

c. To be informed by the Controller or the Data Processor, upon request, regarding the use given to their personal data.

d. To file complaints before the Superintendence of Industry and Commerce for violations of the provisions of the regulations in force, provided that the internal consultation or complaint process referred to in this Policy Manual is previously exhausted, which, according to the provisions of law, is a procedural requirement.

e. To revoke the authorization and/or request the deletion of the data when the Processing does not respect the constitutional and legal principles, rights and guarantees.

f. Access free of charge to your personal data that have been subject to Processing, under the conditions set forth in this Policy Manual and the law.

g. The right not to be conditioned in any case, for the development of any activity with the Company, to be obliged to provide sensitive personal data.

13. Authorizations and Consent

All the information that **The Company** may collect, store, circulate, use, modify, rectify and/or delete with respect to the owners of the same, must have the express, prior, free and informed consent of the Holder Information.

La Empresa como Responsable del Tratamiento ha elaborado un formato de “Autorización para el Tratamiento de Datos Personales” y ha adoptado procedimientos para solicitarle, a más tardar en el momento de la recolección de sus datos personales. Se entenderá para todos los efectos que la autorización por parte del Titular de la información podrá constar en cualquier medio físico, electrónico, o cualquier medio o instrumento que pueda ser considerado a la luz de la normativa vigente como mensaje de datos, razón por la cual, la autorización podrá provenir de cualquiera de las siguientes fuentes: páginas web, correos electrónicos, llamadas telefónicas, mensajes de texto o cualquier otro formato que permita garantizar su consulta posterior, en ningún caso su silencio será asimilado por La Empresa como una conducta inequívoca. Lo anterior de acuerdo a lo establecido en la Ley 527 de 1999, así como en las normas que la modifiquen, complementen, reglamenten, deroguen o sustituyan.

Una vez conferida la autorización por parte de El Titular de la información, con base en cualquiera de estos mecanismos, La Empresa garantizará a El Titular de la información la posibilidad de poder verificar el estado de la misma en cualquier tiempo. En el Tratamiento de datos personales sensibles, cuando dicho Tratamiento sea posible conforme a lo establecido en el artículo 6 de la Ley 1581 de 2012, La Empresa cumplirá con las siguientes obligaciones:

- Informar al Titular que por tratarse de datos sensibles no está obligado a autorizar su Tratamiento.
- Informar al Titular de forma explícita y previa, además de los requisitos generales de la autorización para la recolección de cualquier tipo de dato personal, cuáles de los datos que serán objeto de Tratamiento son sensibles y la finalidad de su Tratamiento, y además obtener su consentimiento expreso.

The Company as Data Controller has developed an "**Authorization for the Processing of Personal Data**" format and has adopted procedures to request it, at the latest at the time of collection of your personal data. It shall be understood for all purposes that the authorization by the Data Subject may be recorded in any physical, electronic, or any means or instrument that may be considered in light of current regulations as a data message, which is why the authorization may come from any of the following sources: web pages, emails, phone calls, text messages or any other format that allows to guarantee its subsequent consultation, in any case their silence will be assimilated by the Company as an unequivocal conduct. The above in accordance with the provisions of Law 527 of 1999, as well as the rules that modify, supplement, regulate, repeal or replace it.

Once the authorization has been granted by the Data Subject, based on any of these mechanisms, the Company shall guarantee to the Data Subject the possibility of verifying the status of the information at any time. In the Processing of sensitive personal data, when such Processing is possible in accordance with the provisions of Article 6 of Law 1581 of 2012, the Company shall comply with the following obligations:

- Inform the Holder that since it is sensitive data, he/she is not obliged to authorize its Processing.
- Inform the Data Subject explicitly and in advance, in addition to the general requirements of authorization for the collection of any type of personal data, which of the data to be processed are sensitive and the purpose of their processing, and also obtain their express consent.

14. Medidas de seguridad de la información

Givaudan Colombia S.A.S. tendrá protocolos de seguridad de obligatorio cumplimiento para todo el personal que tenga acceso a datos de carácter personal y a los sistemas de información. El procedimiento deberá considerar, como mínimo, los siguientes aspectos: a) Capacitación del personal que ingresa a la organización acerca de la Política de Tratamiento de datos personales y los mecanismos y protocolos de seguridad para el tratamiento de estos. b) Ámbito de aplicación del procedimiento con especificación detallada de los recursos protegidos. c) Medidas, normas, procedimientos, reglas y estándares encaminados a garantizar el nivel de seguridad exigido en la Ley 1581 de 2012 y el Decreto 1377 de 2013. d) Funciones y obligaciones del personal. e) Estructura de las bases de datos de carácter personal y descripción de los sistemas de información que los tratan. f) Procedimiento de notificación, gestión y respuesta ante las incidencias. g) Procedimientos de realización de copias de respaldo y de recuperación de los datos. h) Controles periódicos que se deban realizar para verificar el cumplimiento de lo dispuesto en el procedimiento de seguridad que se implemente. i) Medidas a adoptar cuando un soporte o documento sea transportado, desechado o reutilizado. j) El procedimiento deberá mantenerse actualizado en todo momento y deberá ser revisado siempre que se produzcan cambios relevantes en el sistema de información o en la organización del mismo. k) El contenido del procedimiento deberá adecuarse en todo momento a las disposiciones vigentes en materia de seguridad de los datos personales.

14. Information Security Measures

Givaudan Colombia S.A.S. will have security protocols of mandatory compliance for all personnel who have access to personal data and information systems. The procedure must consider, at least, the following aspects: a) Training of personnel entering the organization about the Policy of Treatment of personal data and security mechanisms and protocols for the treatment of these. b) Scope of application of the procedure with detailed specification of the protected resources. c) Measures, norms, procedures, rules and standards aimed at ensuring the level of security required by Law 1581 of 2012 and Decree 1377 of 2013. d) Roles and obligations of personnel. e) Structure of the personal databases and description of the information systems that process them. f) Procedure for notification, management and response to incidents. g) Procedures for making backup copies and data recovery. h) Periodic controls to be carried out to verify compliance with the provisions of the security procedure to be implemented. i) Measures to be adopted when a medium or document is transported, discarded or reused. j) The procedure shall be kept up to date at all times and shall be reviewed whenever relevant changes occur in the information system or in its organization. k) The content of the procedure shall be adapted at all times to the provisions in force regarding the security of personal data.

15. Consultas y Reclamos por parte del Titular

Los derechos de los Titulares podrán ser ejercidos ante La Empresa por las siguientes personas: **a.** Por el Titular de los datos, quien deberá acreditar ante La Empresa su identidad en forma suficiente por los distintos medios o mecanismos que tenemos a su disposición. **b.** Por los causahabientes del Titular de los datos, quienes deberán acreditar tal calidad ante La Empresa **c.** Por el representante y/o apoderado del Titular de los datos, previa acreditación ante La Empresa de la representación o apoderamiento. **d.** Por estipulación a favor de otro o para otro. De acuerdo con lo previsto en la ley 1581, en sus artículos 14 y 15, para el ejercicio de cualquiera de los derechos que le asisten como Titular de los datos, usted podrá utilizar ante La Empresa cualquiera de los mecanismos que se establecen en el numeral 18 de la presente política.

15.1. Procedimiento para la realización de consultas

Los Titulares o sus causahabientes podrán consultar la información personal del Titular que repose en cualquier base de datos de propiedad de **La Empresa**. Por su parte, **La Empresa** o Encargado del Tratamiento deberán suministrar a estos toda la información contenida en el registro individual o que esté vinculada con la identificación del Titular.

La consulta se formulará por el medio habilitado por **La Empresa** o Encargado del Tratamiento y debe mantener prueba de esta.

La consulta será atendida en un término máximo de diez (10) días hábiles contados a partir de la fecha de recibo de la misma. Cuando no fuere posible atender la consulta dentro de dicho término, se informará al interesado expresando los motivos de la demora y señalando la fecha en que se atenderá su consulta, la cual en ningún caso podrá superar los cinco (5) días hábiles siguientes al vencimiento del primer término.

Se podrán consultar de forma gratuita los datos personales al menos una vez cada mes calendario, y cada vez que existan

15. Inquiries and Claims by the Data Holder

The rights of the Data Subject may be exercised before The Company by the following persons: a. By the Data Subject, who must prove to The Company his/her identity sufficiently through the different means or mechanisms available to him/her. b. By the successors of the Data Subject, who must prove such capacity before The Company. c. By the representative and/or attorney-in-fact of the Data Subject, prior accreditation before The Company of the representation or power of attorney. d. By stipulation in favor of or for another. In accordance with the provisions of Law 1581, in Articles 14 and 15, for the exercise of any of the rights you have as a Data Subject, you may use any of the mechanisms established in paragraph 18 of this policy before The Company.

15.1. Procedure for making inquiries

The Data Holders or their assignees may consult the personal information of the Data Holder contained in any database owned by **The Company**. For their part, **The Company** or the Data Processor shall provide them with all the information contained in the individual record or that is linked to the identification of the Data Holder.

The consultation shall be made by the means enabled by **The Company** or the Data Processor and proof of this must be kept.

The consultation will be answered within a maximum term of ten (10) working days from the date of receipt thereof. When it is not possible to answer the consultation within such term, the interested party will be informed stating the reasons for the delay and indicating the date on which the consultation will be

modificaciones sustanciales de las Políticas establecidas en este Manual que motiven nuevas consultas.

Para consultas cuya periodicidad sea mayor a una por cada mes calendario, La Empresa podrá cobrar al Titular los gastos de envío, reproducción y, en su caso, certificación de documentos.

15.2.Procedimiento para la realización de reclamos

El Titular o sus causahabientes que consideren que la información contenida en una base de datos debe ser objeto de corrección, actualización o supresión, podrán presentar un reclamo ante **La Empresa** o el Encargado del Tratamiento el cual será tramitado bajo las siguientes reglas:

15.2.1. El reclamo se formulará mediante solicitud dirigida a **La Empresa** o al Encargado del Tratamiento con la identificación del Titular, la descripción de los hechos que dan lugar al reclamo, la dirección, y acompañando los documentos que quiera hacer valer. Si el reclamo resulta incompleto, se requerirá al interesado dentro de los cinco (5) días siguientes a la recepción del reclamo para que subsane las fallas. Transcurridos dos (2) meses desde la fecha del requerimiento, sin que el solicitante presente la información requerida, se entenderá que ha desistido del reclamo.

15.2.2. En caso de que quien reciba el reclamo no sea competente para resolverlo, dará traslado a quien corresponda en un término máximo de dos (2) días hábiles e informará de la situación al interesado.

15.2.3. Una vez recibido el reclamo completo, se incluirá en la base de datos una leyenda que diga "reclamo en trámite" y el motivo del mismo, en un término no mayor a dos (2) días hábiles. Dicha leyenda deberá mantenerse hasta que el reclamo sea decidido.

15.2.4. El término máximo para atender el reclamo será de quince (15) días hábiles contados a partir del día siguiente a la fecha de su recibo. Cuando no fuere

answered, which in no case may exceed five (5) working days following the expiration of the first term.

Personal data may be consulted free of charge at least once every calendar month, and every time there are substantial modifications to the Policies set forth in this Manual that motivate new consultations.

For consultations whose frequency is greater than one per calendar month, the Company may charge the Holder the costs of shipping, reproduction and, where appropriate, certification of documents.

15.2.Procedure for making claims

The Data Holder or his/her assignees who consider that the information contained in a database should be corrected, updated or deleted, may file a claim with The Company or the Data Processor, which shall be processed under the following rules:

15.2.1. The claim shall be formulated by means of a request addressed to The Company or the Data Processor with the identification of the Data Subject, the description of the facts giving rise to the claim, the address, and accompanied by the documents he/she wishes to assert. If the claim is incomplete, the interested party will be required within five (5) days after receipt of the claim to correct the faults. After two (2) months from the date of the requirement, without the applicant submitting the required information, it shall be understood that the claim has been abandoned.

15.2.2. In the event that the person receiving the claim is not competent to resolve it, he/she shall transfer it to the appropriate person within a maximum term of two (2) business

posible atender el reclamo dentro de dicho término, se informará al interesado los motivos de la demora y la fecha en que se atenderá su reclamo, la cual en ningún caso podrá superar los ocho (8) días hábiles siguientes al vencimiento del primer término.

15.3. Supresión de la Información

El Titular de la información podrá en cualquier tiempo, solicitar a **La Empresa** la supresión de sus datos personales, siempre que:

15.3.1. En el tratamiento no se respeten los principios, derechos y garantías constitucionales y legales.

15.3.2. Cuando la Superintendencia de Industria y Comercio así lo determine.

Sin perjuicio de lo anterior, es preciso tomar en consideración que **La Empresa** solamente podrá suprimir la información de El Titular, siempre que ello no conlleve al incumplimiento de normas legales y/u obligaciones que le competan conforme a la normatividad vigente. Valga decir, no podrán ser objeto de supresión los datos de El Titular, cuando quiera que:

15.3.3. El Titular de la información tenga un deber legal o contractual con **La Empresa** y, para lograr su cabal cumplimiento se requiera la información que consta en la base de datos.

days and inform the interested party of the situation.

15.2.3. Once the complete claim has been received, a legend will be included in the database stating "claim in process" and the reason for the claim, within a term not exceeding two (2) business days. Said legend shall be maintained until the claim is decided.

15.2.4. The maximum term to address the claim will be fifteen (15) working days from the day following the date of receipt. When it is not possible to address the claim within such term, the interested party shall be informed of the reasons for the delay and the date on which the claim will be addressed, which in no case may exceed eight (8) business days following the expiration of the first term.

15.3. Deletion of Information

The Holder of the information may at any time request The Company to delete his/her personal data, provided that:

15.3.1. In the processing, the constitutional and legal principles, rights and guarantees are not respected.

15.3.2. When the Superintendence of Industry and Commerce so determines.

Notwithstanding the foregoing, it is necessary to take into consideration that The Company may only delete the information of The Holder, provided that this does not lead to non-compliance with legal regulations and/or obligations under the regulations in force. In other words, the data of the Data Holder shall not be subject to deletion, whenever:

15.3.3. The Holder of the information has a legal or contractual duty with The Company

15.3.4. La supresión de los datos por parte de **La Empresa**, implique la obstaculización del desarrollo de las investigaciones judiciales a ejecutar por parte de las autoridades competentes.

15.4. Revocación de la Autorización

El Titular de la Información podrá en cualquier tiempo revocar la autorización conferida a **La Empresa** para el tratamiento de sus datos personales. Para estos efectos, **La Empresa** creará mecanismos que permitan a El Titular de la Información revocar la autorización conferida. Estos mecanismos deberán ser de fácil acceso y, serán gratuitos en los casos que establece la ley.

and, in order to achieve its full compliance, the information contained in the database is required.

15.3.4. The suppression of the data by The Company implies the hindering of the development of the judicial investigations to be carried out by the competent authorities.

15.4. Revocation of Authorization

The Data Holder may at any time revoke the authorization granted to The Company for the processing of his/her personal data. For these purposes, **The Company** will create mechanisms that allow the Data Holder to revoke the authorization granted. These mechanisms shall be easily accessible and, in the cases established by law, shall be free of charge.

16. Contacto

Los derechos de los titulares podrán ser ejercidos a través de los canales que han sido habilitados por **La Empresa** para dicho efecto, los cuales se encuentran a su disposición de forma gratuita, así:

- Teléfono: (1) 4252935 en la ciudad de Bogotá
- Dirección: Carrera 98 No. 25G - 40 en Bogotá Colombia
- Correo electrónico: francisco.alarcon@givaudan.com; Esta dirección de correo electrónico está siendo protegida contra los robots de spam. Necesita tener JavaScript habilitado para poder verlo.
- Enlace: <https://www.givaudan.com/specials/colombia-legal-compliance>]

16. Contact

The rights of the holders may be exercised through the channels that have been enabled by the Company for this purpose, which are available free of charge, as follows:

- Telephone: (1) 4252935 in the city of Bogotá.
- Address: Carrera 98 No. 25G - 40 in Bogotá Colombia.
- E-mail francisco.alarcon@givaudan.com; This email address is being protected from spambots. You need JavaScript enabled to view it.
- Link: <https://www.givaudan.com/specials/colombia-legal-compliance>]

Servicio al Cliente en el horario: De lunes a viernes entre de 08:00 a.m. a 12:00 m. y de 02:00 p.m. a 06:00 p.m., el cual sólo estará habilitado para el trámite de consultas.

Customer Service during the following hours: Monday to Friday from 08:00 a.m. to 12:00 m. and from 02:00 p.m. to 06:00 p.m., which will only be available for inquiries.

17. Modificación de la Política de tratamiento

Givaudan Colombia S.A.S. se reserva el derecho de modificar esta Política de Tratamiento de la Información y de Datos Personales en su totalidad o parcialmente. En caso de presentarse cambios sustanciales en el contenido de este Manual de Políticas de Tratamiento de Datos Personales informará a los titulares de Datos sobre dichos cambios antes o a más tardar al momento de la implementación de las nuevas políticas. Las modificaciones se publicarán y comunicarán por medio de <https://www.givaudan.com/specials/colombia-legal-compliance> bajo el enlace “Política de tratamiento de datos personales”.

Además, cuando el cambio se refiera a la finalidad del Tratamiento de los datos personales, La Empresa obtendrá una nueva autorización de parte de los titulares.

17. Modifications to this policy

- **Givaudan Colombia S.A.S.** reserves the right to modify this Information and Personal Data Processing Policy in whole or in part. In the event of substantial changes in the content of this Manual of Personal Data Processing Policies, it will inform the Data owners about such changes before or at the latest at the time of the implementation of the new policies. The changes will be published and communicated through our <https://www.givaudan.com/specials/colombia-legal-compliance>

under the link "Personal Data Processing Policy".

In addition, when the change refers to the purpose of the processing of personal data, **The Company** will obtain a new authorization from the data subjects.

18. Entrada en vigencia de la Política de Tratamiento

La presente Política de Tratamiento de Datos Personales fue creada el 30 de abril de 2017 y actualizada el día treinta (30) del mes de agosto del año dos mil veintitrés (2023) y empieza a regir a partir del primero (1) de diciembre del año dos mil veintitrés (2023).

MIGUEL PRADILLA

Representante Legal

GIVAUDAN COLOMBIA S.A.S.

Versión	Fecha
1	30/04/2017
2	30/08/2023

REGISTRO DE ACTUALIZACIONES

Fecha	Concepto	Revisa	Aprueba
30/08/2023	Actualización del Manual de política de tratamiento de datos personales	Francisco Alarcón	Miguel Pradilla

18. Validity

The present Personal Data Processing Policy was created on April 30, 2017, and was updated on August thirty (30), two thousand and twenty-three (2023) and becomes effective as of December first (1), two thousand and twenty-three (2023).

MIGUEL PRADILLA

Legal Representative

GIVAUDAN COLOMBIA S.A.S.

Versión	Date	Modifications
1	30/04/2017	Personal data processing policy manual - original document
2	30/08/2023	Modifications regarding the introduction, purpose, scope, addressees, applicable legal framework, definitions, principles, purposes of the databases, information security measures, duties and annexes that are an integral part of the same.

REGISTRO DE ACTUALIZACIONES

Date	Concept	Reviews	Approves
30/08/2023	Actualización del Manual de política de tratamiento de datos personales	Francisco Alarcón	Miguel Pradilla

<p>19. Anexos</p>	<p>19. Annexes</p>
<p>19.1. Aviso de privacidad</p>	<p>19.1. Data privacy</p>
<p>G I V A U D A N C O L O M B I A S . A . S .</p> <p>TRATAMIENTO DE DATOS PERSONALES</p> <p>El presente aviso está dirigido a todos los clientes finales, aspirantes, empleados, exempleados, encuestadores, proveedores, visitantes y demás grupos de interés que tengan relación GIVAUDAN COLOMBIA S.A.S. tanto activos como inactivos (En adelante “Los Titulares”), cuyos datos personales se encuentran incluidos en las bases de datos de la compañía.</p> <p>GIVAUDAN COLOMBIA S.A.S. (En adelante GIVAUDAN), identificada bajo el NIT 830.077.389-1, domiciliada en la ciudad de Bogotá D.C., debidamente constituida conforme a las leyes de la República de Colombia, mediante documento privada inscrito y registrado ante la Cámara de Comercio de Bogotá D.C.</p> <p>INFORMA</p> <ol style="list-style-type: none"> 1. Que la Ley 1581 de 2012, estableció el Régimen General de Protección de Datos Personales; 2. Que mediante el Decreto 1377 de 2013, el cual fue publicado el 27 de junio de 2013, se reglamentó la Ley 1581 de 2012 en materia de protección de datos personales, a efectos de facilitar su implementación y cumplimiento. 3. Que en desarrollo del artículo 25 de la Ley 1581 de 2012, se creó el Registro Nacional de Bases de Datos, y su reglamentación consta en el Decreto Único Reglamentario 1074 de 2015 y la Circular Externa No. 02-2015. 4. Que la información que GIVAUDAN COLOMBIA S.A.S. contiene en sus bases de datos, será utilizada para los siguientes fines: 1. Ejecutar las actividades propias de La Empresa para cumplir su objeto social, todo lo cual se hará con base en la finalidad de la Base de Datos en la que reposan los Datos Personales de los Titulares. 2. Ofrecerle 	<p>G I V A U D A N C O L O M B I A S . A . S .</p> <p>PROCESSING OF PERSONAL DATA</p> <p>This notice is addressed to all end customers, applicants, employees, former employees, surveyors, suppliers, visitors and other stakeholders that have a relationship with GIVAUDAN COLOMBIA S.A.S., both active and inactive (hereinafter "The Holders"), whose personal data are included in the company's databases.</p> <p>GIVAUDAN COLOMBIA S.A.S. (hereinafter GIVAUDAN), identified under NIT 830.077.389-1, domiciled in the city of Bogotá D.C., duly incorporated under the laws of the Republic of Colombia, by means of a private document registered and recorded before the Chamber of Commerce of Bogotá D.C.</p> <p>INFORM</p> <ol style="list-style-type: none"> 1. That Law 1581 of 2012, established the General Regime for the Protection of Personal Data; 2. That by means of Decree 1377 of 2013, which was published on June 27, 2013, Law 1581 of 2012 was regulated in matters of personal data protection, for the purpose of facilitating its implementation and compliance. 3. That in development of Article 25 of Law 1581 of 2012, the National Database Registry was created, and its regulations are contained in the Sole Regulatory Decree 1074 of 2015 and External Circular No. 02-2015.

los productos, servicios y o beneficios que buscan satisfacer las necesidades de los Titulares, o los productos y servicios de La Empresa, lo cual puede hacerse por medios físicos o a través de correos electrónicos y/o terminales móviles. 3. Enviar la información a entidades gubernamentales por exigencia legal. 4. Consultar información en las listas de control (Listas Nacionales e Internacionales), consultar a la CIFIN, a las centrales de información, Lista Clinton, Procuraduría, Contraloría, Policía Nacional, DIJIN con el fin de preservar la confianza y transparencia entre el Titular de los Datos y La Empresa. 5. Soportar procesos de auditoría externa e interna. 6. Para la ejecución de procesos de índole judicial y extrajudicial en los casos permitidos por los Estatutos y Reglamentos de La Empresa. 7. Registrar la información de Empleados, exempleados, proveedores, clientes (activos e inactivos) en las bases de datos de La Empresa, para el envío de información contractual, comercial y obligacional a que hubiere lugar. 8. Para verificación de referencias de empleados, exempleados, proveedores, clientes (activos e inactivos) en las bases de datos. 9. Respecto de la recolección y tratamiento de datos realizados mediante mecanismos automatizados con el objeto de generar registros de actividad de los visitantes y registros de audiencia La Empresa, sólo podrá utilizar dicha información para la elaboración de informes que cumplan con los objetivos señalados. En ningún caso podrá realizar operaciones que impliquen asociar dicha información a algún usuario identificado o identificable. 10. Efectuar encuestas para evaluar las propuestas de fragancias en el desarrollo de los proyectos del negocio; 11. Realizar actividades de publicidad y prospección comercial, así como encuestas de opinión; 12. Efectuar las gestiones pertinentes para el desarrollo del objeto social de la compañía en lo que tiene que ver con el cumplimiento del objeto del contrato celebrado con el Titular de la información; 13. Promoción, selección y gestión de personal; 14. Ofrecer programas de bienestar corporativo y planificar actividades empresariales, para el titular y sus beneficiarios como: fechas especiales, atención a auditorias, procesos administrativos, entre otros; 15. Seguridad y control acceso a edificios; 16. Video vigilancia; 17. Transmitir los datos personales fuera del país a terceros con los cuales Givaudan Colombia S.A.S. haya suscrito un contrato de procesamiento de datos y sea necesario entregársela para el cumplimiento del objeto

4. That the information that **GIVAUDAN COLOMBIA S.A.S.** contains in its databases, will be used for the following purposes: 1. Execute the activities of The Company to fulfill its corporate purpose, all of which will be done based on the purpose of the Database in which the Personal Data of the Data Controllers are stored. 2. To offer the products, services and/or benefits that seek to satisfy the needs of the Data Subjects, or the products and services of The Company, which may be done by physical means or through e-mails and/or mobile terminals. 3. To send the information to governmental entities as required by law. 4. Consult information in the control lists (National and International Lists), consult the CIFIN, information centers, Clinton List, Attorney General's Office, Comptroller's Office, National Police, DIJIN in order to preserve the trust and transparency between the Data Subject and The Company. 5. To support external and internal auditing processes. 6. For the execution of judicial and extrajudicial processes in the cases allowed by the Bylaws and Regulations of The Company. 7. To register the information of Employees, former employees, suppliers, customers (active and inactive) in the Company's databases, for the sending of contractual, commercial and obligatory information as the case may be. 8. For verification of references of employees, former employees, suppliers, customers (active and inactive) in the databases. 9. Regarding the collection and processing of data through automated mechanisms in order to generate records of visitor activity and audience records, The Company may only use such information for the preparation of reports that meet the stated objectives. Under no circumstances may it carry out operations that imply associating said information to any identified or identifiable user. 10. Conduct surveys to evaluate fragrance proposals in the development of business projects; 11. To carry out advertising and commercial prospecting activities, as well as opinion polls; 12. To carry out the pertinent actions for the development of the company's corporate purpose in relation to the fulfillment of the purpose of the contract entered into with the Data Subject; 13.

contractual; 18. Contactar al titular a través de correo electrónico para el envío de extractos, estados de cuenta o facturas en relación con las obligaciones derivadas del contrato celebrado entre las partes; 19. Gestión contable, fiscal y administrativa de proveedores y clientes; 20. Contactar al titular a través de medios telefónicos para realizar encuestas, estudios y/o confirmación de datos personales necesarios para la ejecución de una relación contractual.

5. Que de conformidad a lo establecido en la legislación vigente, **Los Titulares** podrán ejercer sus derechos de consulta, actualización, supresión o rectificación de la información que consta en las bases de datos de **GIVAUDAN COLOMBIA S.A.S.**, conforme a lo establecido en la Política de Tratamiento de datos, la cual está a disposición en el enlace <https://www.givaudan.com/specials/colombia-legal-compliance> Igualmente, el titular podrá contactar a **GIVAUDAN COLOMBIA S.A.S.** para el ejercicio de sus derechos a través de los siguientes canales:

- Teléfono: (1) 4252935 en la ciudad de Bogotá
- Dirección: Carrera 98 No. 25G - 40 en Bogotá Colombia
- Correo electrónico: francisco.alarcon@givaudan.com ; Esta dirección de correo electrónico está siendo protegida contra los robots de spam. Necesita tener JavaScript habilitado para poder verlo.
- Enlace: <https://www.givaudan.com/specials/colombia-legal-compliance>

Promotion, selection and management of personnel; 14. Offer corporate welfare programs and plan business activities, for the holder and its beneficiaries such as: special dates, attention to audits, administrative processes, among others; 15. Security and building access control; 16. Video surveillance; 17. Transmit personal data outside the country to third parties with whom Givaudan Colombia S.A.S. has entered into a data processing contract and it is necessary to deliver it to them for the fulfillment of the contractual purpose; 18. Contact the holder via e-mail to send statements, account statements or invoices in connection with the obligations arising from the contract entered into between the parties; 19. Accounting, fiscal and administrative management of suppliers and customers; 20. Contacting the holder through telephone means to conduct surveys, studies and/or confirmation of personal data necessary for the execution of a contractual relationship.

5. That in accordance with the provisions of the legislation in force, **the Holders** may exercise their rights of consultation, updating, deletion or rectification of the information contained in the databases of **GIVAUDAN COLOMBIA S.A.S.**, in accordance with the provisions of the Data Processing Policy, which is available in this link <https://www.givaudan.com/specials/colombia-legal-compliance>. Likewise, the holder may contact **GIVAUDAN COLOMBIA S.A.S.** to exercise his/her rights through the following channels:

- Telephone: (1) 4252935 in the city of Bogotá.
- Address: Carrera 98 No. 25G - 40 in Bogotá Colombia.
- E-mail: francisco.alarcon@givaudan.com ; This email address is being protected from spambots. You need JavaScript enabled to view it.
Link: <https://www.givaudan.com/specials/colombia-legal-compliance>

6. Que en caso de usted desee ejercer los derechos que como Titular de la Información se le conceden conforme a la normatividad vigente, podrá presentar su reclamación para el tratamiento de datos personales de conformidad con lo previsto en el artículo 15 de la Ley 1581 de 2012, a través de los siguientes medios:

Dirección Física: carrera 98 No. 25G - 40

Correo Electrónico: francisco.alarcon@givaudan.com

Atentamente,

GIVAUDAN COLOMBIA S.A.S.

6. That in case you wish to exercise the rights granted to you as Owner of the Information in accordance with the regulations in force, you may file a claim for the processing of personal data in accordance with the provisions of Article 15 of Law 1581 of 2012, through the following means:

Address: carrera 98 No. 25G - 40

E-mail: francisco.alarcon@givaudan.com

Cordially,

GIVAUDAN COLOMBIA S.A.S.

19.2. Bases de datos inscritas en el Registro Nacional de Bases de datos

19.2.1. Empleados

Descripción:

Esta Base de Datos es manejada por el área es Recursos Humanos y contiene la información que se recolecta sobre los empleados (vinculados a través de contratos de trabajo), contratistas (vinculados a través de contratos de prestación de servicios) aprendices (vinculados a través de contratos de aprendizaje) y estudiantes en práctica.

Esta base de datos también incluye la información de los empleados retirados con quienes **La Empresa** no tiene un contrato de trabajo vigente.

Contenido:

La información personal contenida en esta Base de Datos contiene los siguientes datos personales: nombres, apellidos, tipo y número de identificación, lugar de expedición, fecha y lugar de nacimiento, estado civil, edad, rango de edad, género, discapacidad, lugar de residencia, dirección, teléfono fijo y celular, ciudad, sueldo, fecha de ingreso, fecha de examen médico, fondo de pensiones, EPS, fondo de cesantías, datos de familiares incluidos los niños, niñas y adolescentes en el primer grado de consanguinidad, registros fotográficos, ocupación, cargo, información académica formal y certificada, nivel de estudios, título obtenido, fecha de terminación, nombre de la institución, otros estudios, idiomas, experiencia laboral, condiciones médicas especiales cargo desempeñado, nombre de la empresa, teléfono, nombre del jefe inmediato, fecha de inicio, fecha de retiro, datos de la persona a contactar en caso de emergencia, nombre, parentesco, empresa, cargo, sección, tipo de vinculación, jornada laboral, salario básico, número de cuenta bancaria para nómina, entidad bancaria y ciudad.

19.2. Databases registered with RNBD

19.2.1. Employees

Description:

This Database is managed by the area is Human Resources and contains the information collected on employees (linked through employment contracts), contractors (linked through service provision contracts) apprentices (linked through apprenticeship contracts) and trainees.

This database also includes information on retired employees with whom The Company does not have a current employment contract.

Content:

The personal information contained in this Database contains the following personal data: first names, last names, type and number of identification, place of issue, date and place of birth, marital status, age, age range, gender, disability, place of residence, address, landline and cell phone, city, salary, date of entry, date of medical examination, pension fund, EPS, severance fund, data of family members including children and adolescents in the first degree of consanguinity, photographic records, occupation, position, formal and certified academic information, level of studies, degree obtained, date of completion, name of the institution, other studies, languages, work experience, special medical conditions, position held, name of the company, telephone, name of immediate supervisor, start date, retirement date, data of the person to contact in case of emergency, name, relationship, company, position, section, type of relationship, working day, basic salary, bank account number for payroll, bank and city.

La empresa también recopila los siguientes datos sensibles: Grupo Sanguíneo, datos médicos información que es suministrada por los colaboradores directamente.

Forma en que se recopilan los datos

La Empresa recoge la información contenida en esta base de datos del proceso de contratación de personal, mediante el diligenciamiento de un formato por parte del empleado a través de la plataforma Engage. Adicionalmente, los Datos son solicitados a los Titulares a través del Contrato laboral o de prestación de servicios y mediante encuestas en Google Forms.

Finalidad

Los datos anteriormente mencionados únicamente se recopilan con el fin de cumplir con las obligaciones derivadas del contrato laboral, dentro de los que están, la atención de solicitudes, la generación de certificados y constancias, la afiliación a las entidades del Sistema de Protección Social, la realización de actividades de Bienestar Laboral, el levantamiento de registros contables, los reportes a autoridades de control y vigilancia, la adopción de medidas tendientes a la prevención de actividades ilícitas, pagar impuestos, comunicación en caso de ausencia, entre otros fines administrativos, comerciales y de contacto.

Los datos sensibles como el grupo sanguíneo u otra información relacionada con la salud del trabajador, se utiliza en casos de emergencia, o para el reporte ante las entidades del Sistema de Seguridad Social en Salud.

Tratamiento

El tratamiento que recibe esta base de datos por parte de **La Empresa** en su condición de responsable y encargada incluye la recolección, almacenamiento, uso, circulación interna y supresión de los datos al inactivarse. Los datos también son utilizados para enviar reportes a las entidades administrativas

The company also collects the following sensitive data: blood group, medical data, information provided directly by employees.

How the data is collected

The Company collects the information contained in this database from the recruitment process, through the completion of a form by the employee through the Engage platform. Additionally, the Data are requested to the Data Holders through the labor or service contract and through surveys in Google Forms.

Purpose

The aforementioned data are only collected in order to comply with the obligations arising from the labor contract, among which are, the attention of requests, the generation of certificates and certificates, the affiliation to the entities of the Social Protection System, the realization of activities of Labor Welfare, the lifting of accounting records, reports to control and surveillance authorities, the adoption of measures aimed at the prevention of illegal activities, paying taxes, communication in case of absence, among other administrative, commercial and contact purposes.

Sensitive data such as blood group or other information related to the worker's health, is used in emergency cases, or for reporting to the entities of the Social Security Health System.

Treatment

The treatment that this database receives by The Company in its capacity as responsible and in charge includes the collection, storage, use, internal circulation and deletion of the data upon inactivation. The data is also used to send reports to the

que lo soliciten, con base en las normas del Sistema de Seguridad Social y complementarias.

La información contenida en esta base de datos se guarda en el sistema SAP de **La Empresa**. También se guarda en el software del proveedor de servicio de nómina y en las carpetas digitales de la compañía

Sobre las medidas de **seguridad**, esta base de datos es manejada sólo por las áreas responsables. La información no es pública, no todos los empleados tienen acceso (los accesos a dichas bases son restringidos), y se hace back up diario de la información del sistema.

Vale la pena destacar que al interior de **La Empresa** es posible eliminar datos por solicitud de sus titulares.

Adicionalmente, esta base de datos cumple con las finalidades generales establecidas en el aparte 11 del presente Manual.

Vigencia

Esta Base de Datos estará vigente mientras exista la relación laboral entre el empleado y La Empresa, y por diez (10) años más contados a partir de la fecha de liquidación del contrato. Sin embargo, para asuntos de aportes a pensiones **La Empresa** conservar en archivo esta información por mínimo por 90 años. Así mismo **La Empresa** conserva la información en un archivo histórico de las personas que han estado vinculadas a **La Empresa**.

19.2.2. Clientes:

Descripción

Todos los clientes de **Givaudan** son personas jurídicas y en ella se guarda información que no es personal. De manera tal que si bien esta base de datos no es sujeta al ámbito de aplicación de la ley, La Empresa ha decidido reportarla por si en un futuro llegan a recopilarse datos personales.

administrative entities that request it, based on the rules of the Social Security System and complementary.

The information contained in this database is stored in the Company's SAP system. It is also stored in the payroll service provider's software and in the company's digital folders.

Regarding security measures, this database is handled only by the responsible areas. The information is not public, not all employees have access (access to these databases is restricted), and the information in the system is backed up daily.

It is worth noting that within The Company it is possible to delete data at the request of its owners.

Additionally, this database complies with the general purposes established in section 11 of this Manual.

Validity

This Database shall be in force as long as the labor relationship between the employee and The Company exists, and for ten (10) more years counted from the date of settlement of the contract. However, for matters of pension contributions, the Company will keep this information on file for at least 90 years. Likewise, the Company keeps the information in a historical file of the people who have been linked to the Company.

19.2.2. Customers:

Description

All of Givaudan's customers are legal entities and non-personal information is stored in this database. Therefore, although this database is not subject to the scope of application of the law, the Company has

Esta base de datos corresponde a la información de los clientes de La Empresa, es decir corresponde a aquellas personas que adquieren los saborizantes, fragancias y aromas suministrados por La Empresa en desarrollo de su objeto social.

Esta base de datos es manejada por el Área de Customer Care y por el Área de Sabores y Fragancias.

Contenido

Esta base de datos contiene la siguiente información: Nombre completo, Número de Identificación, dirección, Departamento (estado), Ciudad (municipio), Idioma, Correo electrónico, Actividad Económica, Código CIU, Teléfono Móvil y Teléfono Fijo.

De manera que en un archivo Excel se incluye información con código de cliente, nombre de la organización a la que pertenece, división, si es oficina de Latinoamérica, nombre de la organización, ciudad, término de búsqueda (SearchTerm) y código postal.

Forma en que se recopilan los datos

La información de los clientes es obtenida mediante el diligenciamiento del formato de creación de clientes.

Finalidad

La información contenida en esta base de datos tiene por finalidad permitir a La Empresa cumplir apropiadamente con su objeto social de comercializar saborizantes y aromas, así como las demás actividades análogas prestadas por La Empresa.

De manera que esta base de datos tiene por finalidad la creación mantenimiento, facturación y despacho de productos, así como llevar un control y registro de los clientes que maneja Givaudan y sus respectivos datos de contacto.

decided to report it in case personal data is collected in the future.

This database corresponds to the information of The Company's clients, that is to say, it corresponds to those people who acquire the flavorings, fragrances and aromas supplied by The Company in the development of its corporate purpose.

This database is managed by the Customer Care Area and by the Flavors and Fragrances Area.

Content

This database contains the following information: Full Name, Identification Number, Address, Department (state), City (municipality), Mobile Phone and Landline Phone.

So in an Excel file is included information with client code, name of the organization to which it belongs, division, if it is a Latin American office, name of the organization, city, search term (SearchTerm) and zip code.

How data is collected

Client information is obtained by filling out the client creation form.

Purpose

The information contained in this database is intended to allow the Company to properly comply with its corporate purpose of commercializing flavorings and aromas, as well as other similar activities provided by the Company.

Therefore, the purpose of this database is the creation, maintenance, invoicing and dispatch of products, as well as to keep a control and record of the clients

Tratamiento

La información personal contenida en esta base de datos es objeto de recolección, almacenamiento, uso, circulación interna y supresión de los datos al inactivarse.

La información contenida en esta base de datos se guarda en el sistema SAP de La Empresa.

Sobre las medidas de **seguridad**, se tienen mecanismos y herramientas para que sólo pueda consultar la información quien la crea y quien tiene permiso para uso. De manera que esta base de datos es manejada sólo por las áreas responsables. La información no es pública, no todos los empleados tienen acceso (los accesos a dichas bases son restringidos), y se hace back up diario de la información del sistema.

Vale la pena destacar que al interior de La Empresa es posible eliminar datos por solicitud de sus titulares.

Adicionalmente, esta base de datos cumple con las finalidades generales establecidas en el aparte 10 del presente Manual.

Vigencia

La información personal contenida en esta base de datos es custodiada mientras dura la relación comercial con el cliente más un periodo adicional de 10 años.

Si en un caso individual, existen indicios de una necesidad de protección o de interés histórico de estos datos, se prolongará el plazo de almacenamiento de estos datos hasta que se haya aclarado la necesidad legal de protección.

19.2.3. Proveedores

Descripción

Esta base de datos es manejada por el Área de Compras y corresponde a la información personal que se recolecta sobre las personas naturales que suministran servicios o venden productos a La Empresa.

handled by Givaudan and their respective contact information.

Treatment

The personal information contained in this database is subject to collection, storage, use, internal circulation and deletion of data upon inactivation.

The information contained in this database is stored in the Company's SAP system.

Regarding security measures, there are mechanisms and tools in place so that only those who create the information and those who have permission to use it can consult it. Therefore, this database is handled only by the responsible areas. The information is not public, not all employees have access (access to these databases is restricted), and the information in the system is backed up daily.

It is worth noting that within the Company it is possible to delete data at the request of its owners.

Additionally, this database complies with the general purposes established in section 10 of this Manual.

Validity

The personal information contained in this database is kept for the duration of the commercial relationship with the client plus an additional period of 10 years.

If in an individual case, there are indications of a need for protection or historical interest of this data, the storage period of this data will be extended until the legal need for protection has been clarified.

19.2.3. Suppliers

Description

This database is managed by the Purchasing Area and corresponds to the personal information collected on

Contenido

Esta base de datos contiene la siguiente información: Nombre completo, documento de identificación, dirección, número telefónico, información bancaria, información tributaria, nombre del representante legal, tipo y número de identificación, lugar y fecha de nacimiento, dirección, correo electrónico, teléfono y ocupación.

Forma en que se recopilan los datos

La información primordialmente se obtiene a través de a través del Formulario de Alta de proveedores, a través del RUT, de la información del Certificado de Existencia y Representación Legal de la Cámara de Comercio, Certificación bancaria, Declaración de Lavado de Activos, Financiación del terrorismo LA/FT firmada por representante legal, de la copia del documento de identificación.

En este formulario y declaración el proveedor autoriza para verificar la información suministrada, reportar, almacenar, actualizar, consultar, procesar, compilar, intercambiar, suministrar, grabar, solicitar y divulgar la información de carácter personal ante cualquier operador, centrales de información del Sector Financiero con fines estadísticos, de control, supervisión, pruebas de mercadeo, actualización o verificación información de conformidad con lo preceptuado en la ley de habeas data y de protección de datos personales.

Finalidad

La información contenida en esta base de datos tiene por finalidad crear al proveedor en el sistema de La Empresa, realizar actividades de mantenimiento, compras de bienes y servicios y en general cumplir con las obligaciones derivadas de la relación comercial, realizar pagos, realizar transferencias bancarias asociadas a los servicios prestados o productos vendidos a La Empresa, presentación de información exógena a la DIAN y Secretaria de Hacienda, de

the natural persons who provide services or sell products to The Company.

Content

This database contains the following information: Full name, identification document, address, address, telephone number, bank information, tax information, name of legal representative, type and number of identification, place and date of birth, address, e-mail, telephone and occupation.

How the data is collected

The information is obtained primarily through the Supplier Registration Form, through the RUT, information from the Certificate of Existence and Legal Representation of the Chamber of Commerce, Bank Certification, Declaration of Money Laundering, Financing of Terrorism LA/FT signed by legal representative, copy of the identification document.

In this form and declaration the provider authorizes to verify the information provided, report, store, update, consult, process, compile, exchange, supply, record, request and disclose personal information to any operator, information centers of the Financial Sector for statistical purposes, control, supervision, marketing tests, updating or verification of information in accordance with the provisions of the law of habeas data and protection of personal data.

Purpose

The information contained in this database is intended to create the supplier in the Company's system, perform maintenance activities, purchases of goods and services and in general comply with the obligations arising from the business relationship, make payments, make bank transfers associated with the services provided or products sold to the Company, submission of exogenous information to the DIAN and Secretary

conformidad con lo dispuesto en la normatividad colombiana y contactarlos para contratar de nuevo.

La Base de Datos de Proveedores también puede ser utilizada para dar cumplimiento a las obligaciones contraídas con proveedores así como evaluar la calidad de productos y servicios.

Tratamiento

La información personal contenida en esta base de datos es objeto de recolección, almacenamiento, uso, circulación interna y supresión de los datos al inactivarse.

La información contenida en esta base de datos se guarda en el sistema SAP de La Empresa.

Sobre las medidas de **seguridad**, esta base de datos es manejada sólo por las áreas responsables. La información no es pública, no todos los empleados tienen acceso (los accesos a dichas bases son restringidos), y se hace back up diario de la información del sistema.

Vale la pena destacar que al interior de La Empresa es posible eliminar datos por solicitud de sus titulares.

Adicionalmente, esta base de datos cumple con las finalidades generales establecidas en el aparte 10 del presente Manual.

Vigencia

Esta base de datos se encuentra vigente mientras exista la relación comercial con el proveedor más un periodo adicional de 10 años. Así mismo se conserva un archivo histórico de los proveedores que han estado vinculados con LA EMPRESA.

19.2.4. Aspirantes:

Descripción:

Esta Base de Datos contiene la información que se recolecta sobre los aspirantes a cargos con La Empresa y es manejada por el área de Recursos Humanos.

of Finance, in accordance with the provisions of Colombian regulations and contact them to hire again.

The Suppliers Database may also be used to comply with the obligations contracted with suppliers as well as to evaluate the quality of products and services.

Treatment

The personal information contained in this database is subject to collection, storage, use, internal circulation and deletion of the data upon inactivation.

The information contained in this database is stored in the Company's SAP system.

Regarding security measures, this database is handled only by the responsible areas. The information is not public, not all employees have access (access to these databases is restricted), and the information in the system is backed up daily.

It is worth noting that within the Company it is possible to delete data at the request of its owners.

Additionally, this database complies with the general purposes established in section 10 of this Manual.

Validity

This database is valid as long as the commercial relationship with the supplier exists plus an additional period of 10 years. Likewise, a historical file of the suppliers that have been linked to the COMPANY is kept.

19.2.4. Applicants:

Description:

This Database contains the information collected on applicants for positions with The Company and is managed by the Human Resources area.

Contenido:

La información personal contenida en esta Base de Datos contiene los siguientes datos personales necesarios para ser aspirantes a ser contratados por La Empresa: nombre, teléfonos, correo electrónico, dirección, referencias, experiencia laboral en Givaudan (si aplica), empleo anterior, idiomas, código postal, ciudad, movilidad geográfica, provincia o estado, idioma preferido, país, área funcional preferida, número de móvil privado, aspiraciones profesionales, dirección de correo electrónico de inicio de sesión externo, máxima educación alcanzada, departamento.

Forma en que se recopilan los datos

El área de Recursos Humanos recoge la información contenida en esta base de datos de los procesos de selección y cuando hay una vacante se guardan en "engage" que es un sistema interno en donde se clasifican por nombre y datos básicos del aspirante, así como a través de portales de empleo.

Finalidad

Los datos anteriormente mencionados únicamente se recopilan con el fin de crear al aspirante para su eventual contratación laboral con La Empresa, así como para preseleccionar a un cargo determinado cuando es requerido.

Tratamiento

El tratamiento que recibe esta base de datos por parte de La Empresa en su condición de responsable y encargada incluye el procesamiento de la información de todos los aspirantes para laborar en Givaudan con el fin de preseleccionar a un cargo determinado cuando es requerido. De manera que el tratamiento incluye el procesamiento en un archivo físico y electrónico, la recolección, el almacenamiento, el uso, la circulación y la actualización.

Content:

The personal information contained in this Database contains the following personal data required to be an applicant for employment with The Company: name, telephone numbers, email address, address, references, work experience at Givaudan (if applicable), previous employment, languages, zip code, city, geographic mobility, province or state, preferred language, country, preferred functional area, private mobile number, career aspirations, external login email address, highest education attained, department.

How the data is collected

The Human Resources area collects the information contained in this database from the selection processes and when there is a vacancy it is stored in "engage" which is an internal system where it is classified by name and basic data of the applicant, as well as through employment portals.

Purpose

The aforementioned data is collected solely for the purpose of creating the applicant for eventual employment with the Company, as well as to pre-select for a specific position when required.

Treatment

The treatment that this database receives by The Company in its condition of responsible and in charge includes the processing of the information of all the applicants to work in Givaudan in order to pre-select them to a specific position when required. Thus, the processing includes processing in a physical and electronic file, collection, storage, use, circulation and updating.

Regarding security measures, this database is only handled by the human resources area. It is also

En cuanto a las medidas de seguridad, esta base de datos sólo es manejada por el área de recursos humanos. También es importante destacar que la información no se utiliza para ofrecer servicios o productos de terceros. La información contenida en esta base de datos es de uso exclusivo de **La Empresa** y puede ser suprimida, de acuerdo con lo regulado por la ley al respecto.

Adicionalmente, esta base de datos cumple con las finalidades generales establecidas en el aparte 11 del presente Manual.

Vigencia

Esta Base de Datos estará vigente durante la vigencia de Givaudan.

19.2.5. Visitantes

Descripción:

Esta base de datos corresponde a los visitantes que ingresan a La Empresa.

Contenido:

Esta base de datos contiene la siguiente información personal: Nombres y apellidos, tipo y número de documento de identidad, empresa de donde viene, ARL, foto y huella, documento y dependencia del empleado a quien visita, fecha y hora de entrada, fecha y hora de salida y número de tarjeta de ingreso entregada.

Forma en que se recopilan los datos

Cada visitante debe acercarse a la recepción de la compañía y la persona que esté de turno lo registra en el computador.

Finalidad

La información contenida en esta base de datos tiene por finalidad administrar el ingreso de personal externo a las instalaciones de la compañía, con el objeto de controlar la seguridad dentro de la misma.

important to note that the information is not used to offer services or products of third parties. The information contained in this database is for the exclusive use of The Company and may be deleted, in accordance with the law.

Additionally, this database complies with the general purposes established in section 11 of this Manual.

Validity

This Database will be in effect for the duration of Givaudan.

19.2.5. Visitors

Description:

This database corresponds to visitors who enter The Company.

Content:

This database contains the following personal information: Names and surnames, type and number of identity document, company from which they come, ARL, photo and fingerprint, document and dependency of the employee they visit, date and time of entry, date and time of exit and number of admission card given.

How data is collected

Each visitor must go to the company's reception desk and the person on duty registers it in the computer.

Purpose

The purpose of the information contained in this database is to manage the entry of external personnel to the company's facilities, in order to control security within the company.

Tratamiento

La información personal contenida en esta base de datos es objeto de recolección, almacenamiento, uso y circulación interna y supresión. Esta información se encuentra contenida en los archivos físicos y electrónicos del área de seguridad de la compañía.

Adicionalmente, esta base de datos cumple con las finalidades generales establecidas en el aparte 11 del presente Manual.

Vigencia

Esta Base de Datos estará vigente hasta diez años con posterioridad de la visita. Asimismo, La Empresa conserva la información física en un archivo histórico de las personas que han visitado La Empresa.

19.2.6. Circuito Cerrado de TV

Descripción:

Esta base de datos corresponde a los visitantes que ingresan a La Empresa y quedan registrados mediante video vigilancia.

Contenido:

Esta base de datos contiene la siguiente información personal: registro fílmico de cada visitante.

Forma en que se recopilan los datos

Cada visitante otorga la respectiva autorización cuando ingresa al edificio luego de divisar los letreros que informan la videovigilancia que se realiza.

Finalidad

La información contenida en esta base de datos tiene por finalidad administrar el ingreso de personal externo a las

Treatment

The personal information contained in this database is subject to collection, storage, use and internal circulation and suppression. This information is contained in the physical and electronic files of the company's security area.

Additionally, this database complies with the general purposes established in section 11 of this Manual.

Validity

This Database will be valid for up to ten years after the visit. Likewise, The Company keeps the physical information in a historical file of the people who have visited The Company.

19.2.6. Closed Circuit TV

Description:

This database corresponds to visitors who enter The Company and are recorded through video surveillance.

Content:

This database contains the following personal information: filmic record of each visitor.

Form in which the data is collected

Each visitor grants the respective authorization when he/she enters the building after seeing the signs informing about the video surveillance being carried out.

instalaciones de la compañía, con el objeto de controlar la seguridad dentro de la misma.

Tratamiento

La información personal contenida en esta base de datos es objeto de recolección, almacenamiento, uso y circulación interna y supresión. Esta información se encuentra contenida en los archivos digitales del área de seguridad de la compañía.

Adicionalmente, esta base de datos cumple con las finalidades generales establecidas en el aparte 11 del presente Manual.

Vigencia

Esta Base de Datos estará vigente hasta 30 días con posterioridad de la visita.

19.2.7. Friends Panel fragancias

Descripción:

Esta base de datos corresponde a las personas registradas para realizar encuestas, evaluar propuestas de fragancias en el desarrollo de los proyectos del negocio de Givaudan.

Contenido:

Esta base de datos contiene la siguiente información personal: referido, nombre, habeas data, información actualizada, sexo, celular, correo electrónico, dirección, estrato socioeconómico, estado civil, no. De hijos, ocupación, edad, fecha actualización, estado de salud, alergias, productos que le disgustan, fumador(a), EPS, conceptos de finalidades y preferencias de consumo de productos específicos.

Purpose

The purpose of the information contained in this database is to manage the entry of external personnel to the company's facilities, in order to control security within the company.

Treatment

The personal information contained in this database is subject to collection, storage, use and internal circulation and suppression. This information is contained in the digital files of the company's security area.

Additionally, this database complies with the general purposes established in section 11 of this Manual.

Validity

This database will be valid for up to 30 days after the visit. Likewise, The Company keeps the digital information in a historical file of the people who have visited The Company.

19.2.7. Friends Fragrance Panel

Description:

This database corresponds to people registered to conduct surveys, evaluate fragrance proposals in the development of Givaudan business projects.

Content:

This database contains the following personal information: referrer, name, habeas data, updated information, sex, cell phone, email, address, socioeconomic stratum, marital status, no. Of children, occupation, age, date updated, health status, allergies, products you dislike, smoker, EPS, concepts of purposes and consumption preferences of specific products.

Forma en que se recopilan los datos

Cada persona diligencia el formulario disponible en Survey Monkey.

Finalidad

La información contenida en esta base de datos tiene por finalidad realizar encuestas con las personas registradas, para evaluar propuestas de fragancias en el desarrollo de los proyectos del negocio.

Tratamiento

La información personal contenida en esta base de datos es objeto de recolección, almacenamiento, uso y circulación interna y supresión. Esta información se encuentra contenida en los archivos físicos y electrónicos del área CMI - F&B de la compañía.

Adicionalmente, esta base de datos cumple con las finalidades generales establecidas en el aparte 11 del presente Manual.

Vigencia

Esta Base de Datos estará vigente hasta diez años con posterioridad al diligenciamiento de la encuesta.

How data are collected

Each person fills out the form available on Survey Monkey.

Purpose

The information contained in this database is used to conduct surveys with the registered persons, to evaluate fragrance proposals in the development of business projects.

Treatment

The personal information contained in this database is subject to collection, storage, use and internal circulation and deletion. This information is contained in the physical and electronic files of the CMI - F&B area of the company.

Additionally, this database complies with the general purposes established in section 11 of this Manual.

Validity

This database will be valid for up to ten years after the completion of the survey.

<p>19.3.Procedimiento para la recolección, almacenamiento, uso, circulación y supresión de la información personal de los Titulares.</p>	<p>19.3. Procedures for the collection, storage, use, circulation, and suppression of the personal information of Data Holders.</p>
<p>19.3.1. <u>Finalidades y ámbito de aplicación</u></p> <p>Esta política tiene por finalidad establecer las directrices que “Givaudan”, como responsable y encargado de las Bases de Datos ha de seguir para la recolección, manejo, actualización, rectificación, supresión, transmisión y transferencia y en general el tratamiento de los Datos Personales que le sean entregados o tenga acceso con ocasión al giro ordinario de su objeto social.</p> <p>La presente política deberá ser implementada y aplicada por las áreas responsables de las Bases de Datos al interior de “Givaudan”, así como por los terceros que por su relación con “Givaudan” tenga acceso a las Bases de Datos.</p>	<p>19.3.1. <u>Purpose and scope of application</u></p> <p>The purpose of this policy is to establish the guidelines that " Givaudan ", as responsible and in charge of the Databases, must follow for the collection, handling, updating, rectification, deletion, transmission, and transfer and in general the processing of Personal Data that are delivered or have access to during the ordinary course of its business.</p> <p>This policy must be implemented and applied by the areas responsible for the Databases within "Givaudan", as well as by third parties that by their relationship with " Givaudan" have access to the Databases.</p>
<p>19.3.1.2. <u>Sujeción a los procedimientos.</u></p> <p>Todo empleado, contratistas, dependientes y terceros que por razón a sus funciones y/o actividades al interior “Givaudan” recolecte y/o trate Datos Personales deberá observar los procedimientos, mecanismos, documentos y soportes que el presente manual fija, los cuales deberán ser expuestos de manera clara y precisa al Titular del dato.</p>	<p>19.3.1.2. <u>Submission to procedures.</u></p> <p>All employees, contractors, dependents and third parties that because of their functions or activities in " Givaudan" collects and/or treats Personal Data must observe the procedures, mechanisms, documents and supports that this manual sets, and must be exposed in a clear and precise way to the Owner of the data.</p>
<p>19.3.2. <u>Responsable en el tratamiento de la información. Oficial de privacidad.</u></p> <p>El responsable y encargado para el Tratamiento de las Bases de Datos es: “Givaudan Colombia S.A.S con NIT: 830.077.389-1 Dirección: carrera 98 No. 25G - 40 de la ciudad de Bogotá D.C., Teléfono: (601) 4252935, Oficial de Privacidad: Francisco Alarcón Correo Electrónico: francisco.alarcon@givaudan.com : enlace: https://www.givaudan.com/specials/colombia-legal-compliance</p>	<p>19.3.2. <u>Responsible in the treatment of the information. Data Privacy Officer.</u></p> <p>The responsible and in charge for the Treatment of the Databases is: " Givaudan Colombia S.A.S with NIT: 830.077.389-1 Address: Carrera 98 No. 25G - 40 of the city of Bogotá D.C., Telephone: (601) 4252935, Data Privacy Officer: Francisco Alarcón Email: francisco.alarcon@givaudan.com link: https://www.givaudan.com/specials/colombia-legal-compliance</p>

19.3.3. Condiciones para el tratamiento de datos

19.3.3.1. De la recolección.

“Givaudan” para el desarrollo del giro ordinario de sus negocios, recolectará a través de los mecanismos físicos o tecnológicos los datos personales que considere necesarios y pertinentes, los cuales no podrán ser utilizados para una finalidad distinta a la prevista en el presente Manual o en la Ley. “Givaudan” se abstendrá de utilizar medios engañosos o fraudulentos para la recolección y el tratamiento de datos.

19.3.3.2. De la autorización.

“Givaudan”, adoptará los mecanismos físicos o tecnológicos necesarios que le permitan solicitar y obtener por parte del Titular del dato su autorización, para su recolección y tratamiento.

La autorización deberá ser expresa y clara, y deberá contener como mínimo: los datos objeto de recolección y la finalidad que “Givaudan”, les dará a estos. “Givaudan” podrá obtener la autorización del Titular del dato mediante la implementación de medios tecnológicos que permitan al Titular del dato dar su consentimiento de manera automatizada.

En todo caso, “Givaudan”, podrá obtener la autorización del Titular de dato de manera: i) verbal, ii) por escrito o iii) mediante conductas inequívocas del Titular del dato que permitan concluir de forma razonable que otorgó la autorización. “Givaudan” se abstendrá de recolectar datos sin contar con la debida autorización previa por parte del Titular del mismo.

19.3.3.3. De la revocatoria de la autorización y/o supresión del dato

El Titular del dato podrá en cualquier momento solicitar a “Givaudan” la supresión de sus Datos Personales y/o revocar la autorización para el tratamiento de los datos, mediante la presentación de una petición conforme al procedimiento establecido en el numeral quince de la política de tratamiento

19.3.3. Conditions for data processing

19.3.3.1. Collection.

" For the development of the ordinary course of its business, " Givaudan" will collect by physical or technological methods the personal data that is deemed as necessary and relevant, which may not be used for a purpose other than that provided for in this Manual or in the Law. " Givaudan" will not use any false or fraudulent means for the collection and processing of data.

19.3.3.2. Authorization.

" Givaudan", will adopt all necessary physical or technological mechanisms that allow it to request and obtain authorization from the Data Subject for the collection and processing of the data.

The authorization must contain at least: the data to be collected and the purpose that " Givaudan" will use it for. " Givaudan " can obtain the authorization of the Data Subject through the implementation of technological means that allow the Data Subject to give his consent in an automated way.

In any case, "Givaudan" may obtain the Data Subject's authorization: i) verbally, ii) in writing or iii) through unmistakable behaviors of the Data Subject that allow to reasonably conclude that he/she granted the authorization. " Givaudan" will refrain from collecting data without prior authorization from the Data Subject.

19.3.3.3. Revocation of the authorization or suppression of the data

The Owner of the data can at any time request to " Givaudan" the deletion of its Personal Data as well as the revocation of the authorization for the processing

de datos personales. La solicitud de retiro o revocatoria no procederá cuando el Titular del dato tenga un deber legal o contractual de permanecer en la base de datos.

19.3.3.4. Tratamiento y finalidades a las cuales serán sometidos los datos personales.

Los datos personales que “Givaudan”., conozca dentro del giro ordinario de sus negocios, podrán ser objeto de recolección, almacenamiento, uso, circulación, supresión, transmisión o transferencia, con la finalidad de:

▪ EN CUANTO AL FUNCIONAMIENTO DE “GIVAUDAN”

“Givaudan” con el fin de prestar una mejor información comercial respecto de los servicios y productos ha identificado la necesidad de recolectar y tratar el uso de Datos Personales, para efectos de desarrolla o ejercer su objeto social, y con la finalidad de:

- a. Lograr una eficiente comunicación relacionada con los servicios, productos, necesidades, alianzas, contenidos y para facilitarle el acceso general a la información de interés;
- b. Informar sobre los nuevos productos y/o servicios;
- c. Promover, promocionar y comercializar los productos y/o servicios;
- d. Dar cumplimiento a obligaciones contraídas con nuestros clientes, expositores, compradores profesionales, aliados comerciales, proveedores, accionistas y colaboradores;
- e. Informar sobre cambios de productos y/o servicios;
- f. Evaluar la calidad de los productos y/o servicios, y realizar estudios internos de mercadeo.
- g. Actividades de los programas de fidelización y relacionamiento con los clientes y la comunidad.
- h. Efectuar encuestas para evaluar las propuestas de fragancias en el desarrollo de los proyectos del negocio;

of the data, by submitting a request in accordance with the procedure established in the paragraph fifteen of the personal data processing policy. The request for removal or revocation shall not proceed when the Data Owner has a legal or contractual duty to remain in the database.

19.3.3.4. Treatment and purposes to which personal data will be treated.

The personal data that " Givaudan" obtains in the ordinary course of its business, can be subject of collection, storage, use, circulation, suppression, transmission or transfer, for the following purposes:

▪ REGARDING THE OPERATION OF "GIVAUDAN

" Givaudan" in order to provide better commercial information regarding services and products has identified the need to collect and treat the use of Personal Data, for the purpose of developing or exercising its corporate purpose, and for the purpose of:

- a. To achieve an efficient communication related to services, products, needs, alliances, contents and to facilitate general access to information of interest;
- b. To inform about new products and/or services;
- c. Promote, advertise and market the products and/or services;
- d. To comply with obligations contracted with our clients, exhibitors, professional buyers, commercial allies, suppliers, shareholders and collaborators;
- e. To inform about changes in products and/or services;

- i. Realizar actividades de publicidad y prospección comercial, así como encuestas de opinión;
- j. Efectuar las gestiones pertinentes para el desarrollo del objeto social de la compañía en lo que tiene que ver con el cumplimiento del objeto del contrato celebrado con el Titular de la información;
- k. Promoción, selección y gestión de personal;
- l. e. Ofrecer programas de bienestar corporativo y planificar actividades empresariales, para el titular y sus beneficiarios como: fechas especiales, atención a auditorias, procesos administrativos, entre otros;
- m. Seguridad y control acceso a edificios;
- n. Video vigilancia;
- o. Transmitir los datos personales fuera del país a terceros con los cuales Givaudan Colombia S.A.S. haya suscrito un contrato de procesamiento de datos y sea necesario entregársela para el cumplimiento del objeto contractual;
- p. Contactar al titular a través de correo electrónico para el envío de extractos, estados de cuenta o facturas en relación con las obligaciones derivadas del contrato celebrado entre las partes;
- q. Gestión contable, fiscal y administrativa de proveedores y clientes;
- r. Contactar al titular a través de medios telefónicos para realizar encuestas, estudios y/o confirmación de datos personales necesarios para la ejecución de una relación contractual.

- f. Evaluate the quality of products and/or services, and conduct internal marketing studies.
- g. Activities of the loyalty and relationship programs with customers and the community.
- h. Conduct surveys to evaluate fragrance proposals in the development of business projects;
- i. Carry out advertising and commercial prospecting activities, as well as opinion polls;
- j. Carry out the relevant steps for the development of the corporate purpose of the company in relation to the fulfillment of the purpose of the contract entered into with the Holder of the information;
- k. Promotion, selection and management of personnel;
- l. Offer corporate welfare programs and plan business activities for the holder and its beneficiaries such as: special dates, attention to audits, administrative processes, among others;
- m. Security and control access to buildings;
- n. Video surveillance;
- o. Transmit personal data outside the country to third parties with which Givaudan Colombia S.A.S. has signed a data processing contract and it is necessary to deliver it to them for the fulfillment of the contractual object;
- p. Contact the holder via email to send statements, account statements or invoices in connection with the obligations arising from the contract between the parties;
- q. Accounting, tax and administrative management of suppliers and customers;
- r. Contact the holder through telephone means to conduct surveys, studies and / or confirmation of

	<p>personal data necessary for the execution of a contractual relationship.</p>
<p>19.3.4. <u>Procedimientos</u></p> <p>19.3.4.1. <u>Forma de recolección de los datos</u></p> <p>“Givaudan” por conducto de sus empleados, contratistas o dependientes, podrá recolectar los Datos Personales que considere pertinentes en el giro ordinario de su objeto social, para lo cual podrá utilizar los medios físicos o tecnológicos que considere viables.</p> <p>“Givaudan”, se abstendrán de recolectar Datos Personales sin el consentimiento claro y expreso del Titular de la información, los empleados, contratistas o dependientes de “Givaudan” utilizarán todos los medios dispuestos por “Givaudan” la obtención de la atención de la autorización y la evidencia de la misma. En todo caso, el área Responsable de la recolección del dato deberá garantizar que siempre quede prueba o constancia de la respectiva autorización que emita el Titular del Dato.</p> <p>19.3.4.2. <u>De las bases de datos</u></p> <p>“Givaudan”, ha identificado de manera inicial las siguientes áreas como posibles encargadas de la recolección de los Datos Personales: contabilidad, CMI – F&B, adquisición de talento, recursos humanos, compras, las cuales con el apoyo del área de tecnología deberán implementar las medidas de seguridad que permitan la conservación y custodia de la información de las Bases de Datos que estas manejen.</p> <p>En caso de que las áreas antes mencionadas transmitan o transfieran una base de Datos a otra entidad, deben garantizar que cuentan con la autorización de los titulares para realizar</p>	<p>19.3.4. <u>Procedures</u></p> <p>19.3.4.1. <u>Data collection method</u></p> <p>" Givaudan" may collect Personal Data through its employees, contractors or dependents, as it deems appropriate in the ordinary course of its business, for which it may use physical or technological means it deems feasible.</p> <p>" Givaudan", will not collect Personal Data without the clear and express consent of the Owner of the information, employees, contractors or dependents of " Givaudan" will use all means provided by " Givaudan" to obtain the attention of the authorization and evidence of the same. In any case, the area responsible for the collection of the data shall ensure that there is always proof or evidence of the respective authorization issued by the Data Owner.</p> <p>19.3.4.2. <u>About the databases</u></p> <p>"Givaudan", has initially identified the following areas as possible responsible for the collection of Personal Data: accounting, CMI - F&B, talent acquisition, human resources, human resources, which with the support of the technology area must implement security measures that allow the conservation and custody of the information of the Databases they manage.</p> <p>In the event that the aforementioned areas transmit or transfer a database to another entity, they must</p>

esta acción. Así mismo, estas áreas deben llevar registro de los datos entregados y el nombre de la entidad que los recibió.

Toda entidad que reciba estas Bases de Datos solo podrá usar la información para los propósitos que se encuentran definidos en la autorización otorgada por el Titular de los Datos a "Givaudan".

19.3.4.3. Obligaciones de las áreas responsables.

Son obligaciones de las áreas responsables de los Datos, las siguientes:

- a. Garantizar que la información del Titular sujeta a tratamiento sea veraz, completa, exacta, actualizada, comprobable y comprensible.
- b. Abstenerse de realizar el tratamiento de Datos parciales, incompletos, fraccionados o que induzcan en error.
- c. Realizar oportunamente la actualización, rectificación, o supresión de los Datos Personales.
- d. Velar por la reserva de la información inclusive después de finalizada su relación con alguna de las labores que comprende el tratamiento.
- e. Abstenerse de recolectar, tratar o transmitir Datos Personales de niños, niñas y adolescentes.
- f. Abstenerse de recolectar, tramitar, o transmitir Datos Personales Sensibles, salvo las excepciones previstas por la Ley.
- g. Abstenerse de circular cualquier información que esté siendo controvertida por el Titular y cuyo bloqueo haya sido ordenado por la Superintendencia de Industria y Comercio.
- h. Abstenerse de transferir Datos Personales a países que no proporcionen niveles adecuados de protección de Datos, solo se podrá realizar esta operación cuando se cuente con la autorización del Titular de los Datos.
- i. Avisar a la autoridad en protección de Datos Personales en caso de que se presenten violaciones a los códigos de seguridad y existan riesgos en la administración de la información de los Titulares.

guarantee that they have the authorization of the owners to carry out this action. Likewise, these areas must keep a record of the data delivered and the name of the entity that received them.

Any entity that receives these Databases may only use the information for the purposes that are defined in the authorization given by the Data Subject to "Givaudan".

19.3.4.3. Obligations of the responsible areas.

The following are obligations of the respective areas responsible for the Data:

- a. Ensure that the Data Owner's information subject to processing is truthful, complete, accurate, updated, verifiable and understandable.
- b. Refrain from processing partial, incomplete, fractioned or misleading data.
- c. Timely update, rectification or deletion of Personal Data.
- d. To ensure the confidentiality of the information even after the end of its relationship with any of the tasks included in the processing.
- e. Refrain from collecting, processing or transmitting Personal Data of children and adolescents.
- f. Refrain from collecting, processing or transmitting Sensitive Personal Data, except for the exceptions provided by law.
- g. Refrain from circulating any information that is being disputed by the Data Subject and whose blocking has been ordered by the Superintendence of Industry and Commerce.
- h. Refrain from transferring Personal Data to countries that do not provide adequate levels of data

19.3.4.4. Medidas de seguridad

“Givaudan” mediante el área de Tecnología e Información velará que los Datos Personales, salvo la información pública (nombre, número de cédula de ciudadanía o datos del registro mercantil) no se encuentre disponible en internet u otros medios similares de comunicación, de acuerdo con el Principio de Acceso y Circulación Restringida establecido en la Ley 1581 de 2012.

Las áreas responsables del Tratamiento deben garantizar que la información contenida en sus Bases de Datos, se encuentran bajo las condiciones mínimas de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.

protection; this operation may only be carried out with the authorization of the Data Subject.

- i. Notify the authority in protection of Personal Data in case of violations to the security codes and risks in the administration of the information of the Data Owners.

19.3.4.4. Security and Safety Measures

" Givaudan" through the area of Technology and Information will ensure that Personal Data, except for public information (name, citizenship card number or data from the commercial registry) is not available on the Internet or other similar means of communication, in accordance with the Principle of Access and Restricted Circulation established in Law 1581 of 2012.

The areas responsible for Data Processing must guarantee that the information contained in their Databases is under the minimum security conditions necessary to prevent its adulteration, loss, consultation, use or unauthorized or fraudulent access.

19.3.5. Procedimiento de borrado seguro y supresión de información.

19.3.5.1. Objetivo.

Definir las directrices para el borrado seguro de la información en "Givaudan", a través de la descripción de las actividades de solicitud, preparación, ejecución e informe del resultado del borrado seguro, con el fin de preservar la confidencialidad de la información.

19.3.5.2. Destinatarios.

Este procedimiento aplica para candidatos externos que se postulen a cargos o empleados de Givaudan, que accedan directa o indirectamente a los servicios ofrecidos a través de la página web de "Givaudan".

19.3.5.3. Definiciones generales.

- **BORRADO SEGURO:** Se refiere al procedimiento necesario para garantizar que la información existente en un medio de almacenamiento no pueda ser recuperada a través de alguna técnica especializada.
- **DISPOSITIVO DE ALMACENAMIENTO:** Se refiere a cualquier elemento que se utiliza para almacenar información tales como, discos duros, memorias USB, entre otros.
- **INFORMACIÓN DIGITAL:** Cualquier tipo de información contenida en un medio digital, bien sea en forma de base de datos, en forma de archivos digitales o de intercambio.
- **LISTA DE ARCHIVOS:** Es un término genérico que referencia al conjunto de elementos que cada sistema de archivos utiliza para guardar, tanto la información que identifica los archivos (nombre, tipo, fecha de creación, etc.), como un índice que recoge la ubicación física del contenido del archivo.

19.3.5. Procedure for secure deletion and suppression of information.

19.3.5.1. Objective.

To define the guidelines for the secure deletion of information in "Givaudan", through the description of the activities of request, preparation, execution and report of the result of the secure deletion, in order to preserve the confidentiality of the information.

19.3.5.2. Recipients of the information

This procedure applies to external candidates applying for positions or employees of Givaudan, who directly or indirectly access the services offered through the "Givaudan" website.

19.3.5.3. General definitions.

- **SECURE DELETION:** Refers to the procedure necessary to guarantee that the existing information in a storage medium cannot be recovered through any specialized technique.
- **STORAGE DEVICE:** Refers to any element used to store information such as hard disks, USB flash drives, among others.
- **DIGITAL INFORMATION:** Any type of information contained in a digital medium, either in the form of a database, in the form of digital files or exchange.
- **FILE LIST:** It is a generic term that refers to the set of elements that each file system uses to store both the information that identifies the files (name, type, creation date, etc.), as well as an index that shows the physical location of the file content.

19.3.5.4. Generalidades

El ciclo de vida de la información, de forma simplificada, consta de tres fases: generación, transformación y destrucción. Toda información tiene una vida útil tanto si está en formato digital (CD, DVD, Flash USB, discos magnéticos, tarjetas de memoria, etc.) como en formatos tradicionales (papel, carpetas, entre otros) o servidores dedicados. Cuando la vida de la información llega a su fin, se deben emplear mecanismos de destrucción y borrado seguro para evitar que esta quede al alcance de terceros.

Con el borrado seguro y destrucción de soportes de información no solo se busca proteger la difusión de información confidencial, sino también proteger la fuga de datos personales de los usuarios que puedan contener los soportes.

Para proteger su información personal, tomamos precauciones razonables y seguimos las mejores prácticas de la industria para asegurarnos de que no haya pérdida de manera inapropiada, mal uso, acceso, divulgación, alteración o destrucción de la misma. Aunque ningún método de transmisión a través de Internet o de almacenamiento electrónico es 100% seguro, seguimos todos los requisitos y condiciones mínimos aceptados por la industria, para garantizar la idoneidad de la información.

Los datos recolectados a los clientes por "Givaudan" en <https://www.givaudan.com/specials/colombia-legal-compliance> quedan almacenados en un servidor dedicado ubicado en Suiza.

El hosting dedicado es un entorno de alojamiento de sitios web que proporciona el nivel más alto de asignación de recursos, privacidad y control. Los servidores dedicados están completamente aislados entre sí, por lo que los usuarios obtienen acceso total para configurar su servidor de la forma que deseen sin afectar a otro usuario o verse afectados por las acciones de otros usuarios. Al tener un servidor dedicado "Givaudan" garantiza una mayor seguridad en línea para todos los usuarios del sitio web.

19.3.5.4. General information

The information life cycle, in simplified form, consists of three phases: generation, transformation and destruction. All information has a useful life whether it is in digital format (CD, DVD, USB Flash, magnetic disks, memory cards, etc.) or in traditional formats (paper, folders, among others) or dedicated servers. When the life of the information comes to an end, destruction and secure deletion mechanisms must be used to prevent it from being accessible to third parties.

The secure deletion and destruction of information media not only seeks to protect the dissemination of confidential information, but also to protect the leakage of users' personal data that may be contained in the media.

To protect the personal information we hold about you, we take reasonable precautions and follow industry best practices to ensure that it is not inappropriately lost, misused, accessed, disclosed, altered or destroyed. Although no method of transmission over the Internet or electronic storage is 100% secure, we follow all industry-accepted minimum requirements and conditions to ensure the suitability of the information.

The data collected from customers by "Givaudan" on the [website https://www.givaudan.com/specials/colombia-legal-compliance](https://www.givaudan.com/specials/colombia-legal-compliance) are stored on a dedicated server located in Switzerland.

Dedicated hosting is a web hosting environment that provides the highest level of resource allocation, privacy and control. Dedicated servers are completely isolated from each other, so users get full access to configure their server the way they want without affecting another user or being affected by the actions

“Givaudan” hace limpieza de servidores periódicamente para que estos no lleguen a su capacidad máxima y/o dejen de funcionar. La limpieza consiste en eliminar las imágenes, diseños y ordenes realizadas por los clientes 6 meses antes a la fecha de realización de la actividad. A excepción de la autorización de manejo y tratamiento de datos personales brindada por el usuario estos datos no quedan almacenados en ningún otro lugar físico o en la nube, son eliminados en su totalidad y ya no queda registro existente de los mismos una vez se ejecuta la actividad de limpieza.

Las bases de datos administradas por “Givaudan” se tratarán de mantener indefinidamente, mientras desarrolle su objeto, y mientras sea necesario para asegurar el cumplimiento de obligaciones de carácter legal, particularmente laboral y contable, pero los datos podrán ser eliminados en cualquier momento a solicitud de su titular o por necesidades de “Givaudan”, en tanto esta solicitud no contraríe una obligación legal de “Givaudan” o una obligación contenida en un contrato entre “Givaudan” y el Titular.

El Titular del dato podrá en cualquier momento solicitar a “Givaudan” la supresión de sus Datos Personales y/o revocar la autorización para el tratamiento de los datos, mediante la presentación de una petición conforme al procedimiento establecido en la presente política. La solicitud de retiro o revocatoria no procederá cuando el Titular del dato tenga un deber legal o contractual de permanecer en la base de datos.

19.3.6. Métodos de borrado seguro de información

- Desmagnetización: La desmagnetización consiste en la exposición de los soportes de almacenamiento a un potente campo magnético, proceso que elimina los datos almacenados en el dispositivo. Este método es válido para la destrucción de datos de los dispositivos magnéticos, por ejemplo, discos duros, disquetes, cintas magnéticas de backup, etc. Cada dispositivo, según su tamaño, forma y el tipo de soporte magnético, necesita de una potencia específica para

of other users. Having a dedicated server " Givaudan" ensures greater online security for all website users.

" Givaudan" cleans servers periodically so that they do not reach their maximum capacity and stop working. The cleaning works as follows every images, designs and orders placed by customers 6 months prior to the date of the activity. Except for the authorization of handling and treatment of personal data provided by the user, these data are not stored in any other physical place or in the cloud, they are eliminated in their entirety and there is no longer any existing record of them once the cleaning activity is executed.

The databases managed by " Givaudan" will be kept indefinitely, as long as it develops its purpose, and as long as necessary to ensure compliance with legal obligations, particularly labor and accounting, but the data may be deleted at any time at the request of the holder or for the needs of " Givaudan", as long as this request does not contravene a legal obligation of " Givaudan" or an obligation contained in a contract between " Givaudan" and the Data Subject.

The Data Owner may at any time request " Givaudan" to remove its Personal Data or/and revoke the authorization for the processing of the data, by submitting a request in accordance with the procedure set forth in this policy. The request for removal or revocation shall not proceed when the Data Subject has a legal or contractual duty to remain in the database.

19.3.6. Methods of secure erasure of information.

- De-magnetization: The demagnetization consists of exposing storage media to a powerful magnetic field, a process that eliminates the data stored on the device. This method is valid for the destruction of data from magnetic devices, e.g. hard disks, floppy disks, magnetic backup tapes, etc. Each device, depending on its size, shape and the type of

<p>asegurar la completa polarización de todas las partículas.</p> <ul style="list-style-type: none"> ▪ <u>Destrucción física</u>: El objetivo de la destrucción física es la inutilización del soporte que almacena la información para evitar la recuperación posterior de los datos que almacena. Existen diferentes tipos de técnicas y procedimientos para la destrucción de medios de almacenamiento. ▪ <u>Ejecución de Script</u>: Se ejecuta un script para eliminar toda la información almacenada por los usuarios en un período razonable anterior a la fecha de realización de la actividad. Una vez ejecutado el script las imágenes, órdenes y diseños creados por los usuarios quedan eliminados en su totalidad del servidor sin respaldo de la información. 	<p>magnetic support, needs a specific power to ensure the complete polarization of all particles.</p> <ul style="list-style-type: none"> • <u>Physical destruction</u>: The purpose of physical destruction is to destroy the medium that stores the information in order to prevent subsequent recovery of the data stored on it. There are different types of techniques and procedures for the destruction of storage media. • <u>Script execution in the Control Panel</u>: it is executed a script to delete all the information stored by the users in a reasonable period prior to the date of the activity. After the completion of the activity, the images, orders and designs created by the users are deleted in their entirety from the server without any backup of the information.
---	--

19.4.Gestión de incidentes de seguridad en el tratamiento de datos personales	19.4. Management of security incidents in the processing of personal data
--	--

<p>19.4.1. Objetivo</p> <p>La presente Política tiene como objeto dar los lineamientos de seguridad de la información sujeta a tratamiento de datos por parte de Givaudan Colombia S.A.S., partiendo de la base que la información se deberá manejar con las medidas técnicas, humanas y administrativas que sean necesarias para otorgar seguridad a los registros evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento. para de esta forma, dar cumplimiento de la ley, políticas y procedimientos de atención de derechos de los titulares que pudiesen llegar a ser víctimas de incidentes de seguridad o que se vean vulnerados en el tratamiento de sus datos personales, para lo cual, Givaudan Colombia S.A.S. se plantea dar cumplimiento a los deberes de conservación de la información y de denuncia a la autoridad, así como al deber y principio de seguridad.</p>	<p>19.4.1. Objective</p> <p>The purpose of this Policy is to provide security guidelines for information subject to data processing by Givaudan Colombia S.A.S., on the basis that the information must be handled with the technical, human and administrative measures that are necessary to provide security to the records avoiding their adulteration, loss, consultation, use or unauthorized or fraudulent access. In this way, to comply with the law, policies and procedures for the attention of the rights of holders who may become victims of security incidents or who are violated in the processing of their personal data, for which Givaudan Colombia S.A.S. intends to comply with the duties of preservation of information and reporting to the authority, as well as the duty and principle of security.</p>
--	--

19.4.2. Deberes y principios rectores de los responsables y encargados de tratamiento de datos.

Esta política contempla como deberes fundamentales de **Givaudan Colombia S.A.S.** en el tratamiento de datos personales, el de seguridad de la información, el de conservación de la información y el de denuncia oportuna a la autoridad.

El principio de deber de seguridad: hace referencia a un criterio eminentemente preventivo que obliga a **Givaudan Colombia S.A.S.**, ya sea en calidad de responsable o encargado de tratamiento de datos personales a adoptar las medidas necesarias para evitar las posibles afectaciones a la seguridad de los datos, no obstante, su carácter eminentemente preventivo, este deber demanda que la entidad se encuentre preparada para mitigar los riesgos y daños que puedan llegar a causarse en los eventos en que las medidas de seguridad preventivas fallen, garantizando así, los derechos y libertades fundamentales de los titulares.

El deber de conservación de la información: gira en torno a la obligación de **Givaudan Colombia S.A.S.** de garantizar la adecuada conservación de la información de los titulares bajo estrictas condiciones de seguridad, las cuales se hacen necesarias a fin de mitigar los riesgos de adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.

El deber de denuncia a la autoridad: entendido como la obligación de **Givaudan Colombia S.A.S.** de informar y denunciar ante la autoridad nacional de protección de datos personales, es decir, ante la Delegatura para la Protección de Datos Personales de la Superintendencia de Industria y Comercio, cualquier violación a los códigos de seguridad o la existencia de cualquier riesgo en la administración de la información de los titulares.

19.4.2. Duties and guiding principles of data controllers and data processors

This policy contemplates as fundamental duties of **Givaudan Colombia S.A.S.** in the treatment of personal data, the security of information, the conservation of information and timely reporting to the authority.

The principle of security duty: refers to an eminently preventive criterion that obliges **Givaudan Colombia S.A.S.**, either as controller or processor of the processing of personal data, to adopt the necessary measures to avoid the possible affectations to the security of the data, notwithstanding, its eminently preventive character, this duty demands that the entity is prepared to mitigate the risks and damages that may be caused in the events in which the preventive security measures fail, thus guaranteeing the fundamental rights and freedoms of the holders.

The duty to preserve the information: Givaudan Colombia S.A.S. has the obligation to guarantee the adequate preservation of the information of the holders under strict security conditions, which are necessary in order to mitigate the risks of adulteration, loss, consultation, use or unauthorized or fraudulent access.

The duty to report to the authority: understood as the obligation of **Givaudan Colombia S.A.S.** to inform and report to the national authority for the protection of personal data, that is, to the Delegation for the Protection of Personal Data of the Superintendence of Industry and Commerce, any violation to the security codes or the existence of any risk in the administration of the information of the holders.

19.4.3. Reporte de incidentes de seguridad en el marco del contrato de encargatura de datos.

Cualquier persona natural o jurídica que suscriba un contrato de encargatura de datos con **Givaudan Colombia S.A.S.** que implique la realización de cualquier actividad que involucre el tratamiento de datos personales, se someterá al cumplimiento de la política establecida en el presente documento, siéndole exigible el cumplimiento de los deberes y obligaciones que conlleva ser encargado del tratamiento de datos personales para **Givaudan Colombia S.A.S.**

En virtud de lo antes expuesto, el presente documento deberá incluirse como documento anexo a todos los contratos de encargatura de datos o transmisión que llegue a celebrar **Givaudan Colombia S.A.S.**, así mismo, se pactará dentro de estos contratos como obligación del encargado, el notificar sin dilación alguna los incidentes de seguridad que involucren los datos personales transmitidos, con la finalidad de que se conozca inmediatamente el incidente y se puedan activar las medidas oportunas; no obstante, la práctica de la notificación antes descrita no exime al encargado del deber de notificar el incidente de seguridad a la Delegatura para Asuntos Jurisdiccionales de la Superintendencia de Industria y Comercio, de conformidad a lo estipulado en el literal k del artículo 18 de la ley 1581 de 2012.

Adicionalmente, el contrato de transmisión o de encargatura de datos debe establecer como mínimo los siguientes aspectos:

1. Protocolo de respuesta en el manejo de incidentes de seguridad.
2. Roles y responsabilidades de los intervinientes en el contrato.
3. Datos de contacto de los supervisores del contrato, siendo al menos un funcionario por cada entidad interviniente.

19.4.3. Reporting of security incidents within the framework of the data entrustment contract

Any natural or legal person who enters into a data processing contract with **Givaudan Colombia S.A.S.** that involves the performance of any activity that involves the processing of personal data, shall be subject to compliance with the policy established in this document, and shall be required to comply with the duties and obligations of the processor of the processing of personal data for **Givaudan Colombia S.A.S.**

By virtue of the foregoing, this document shall be included as an annex to all data entrustment or transmission contracts entered into by **Givaudan Colombia S.A.S.**, likewise, it shall be agreed within these contracts as an obligation of the processor, to notify without delay any security incidents involving personal data transmitted, in order that the incident is immediately known and the appropriate measures can be activated; however, the practice of the notification described above does not relieve the processor of the duty to notify the security incident to the Delegation for Jurisdictional Affairs of the Superintendence of Industry and Commerce, in accordance with the provisions of paragraph k of Article 18 of Law 1581 of 2012.

In addition, the data transmission or entrustment contract must establish at least the following aspects:

1. Response protocol in the management of security incidents.
2. Roles and responsibilities of those involved in the contract.
3. Contact details of the contract supervisors, being at least one official for each intervening entity.

4. El procedimiento para el trámite de las consultas e inquietudes que puedan presentar los titulares de la información.
5. Deberá establecerse la forma en que se realizará el reporte de los incidentes de seguridad en caso de existir sub encargos por parte del encargado del tratamiento.
6. La obligación expresa de cumplir las políticas de tratamiento de información.

19.4.4. Conservación de registros internos.

Givaudan Colombia S.A.S. guardará soporte documental, independientemente del formato, sea virtual o en físico, de todos los aspectos de cada incidente de seguridad que se presente, con la finalidad de demostrar el cumplimiento del régimen de protección de datos personales en caso de la apertura de alguna investigación administrativa por tal motivo, al tiempo que, dichos registros serán utilizados con la finalidad de crear matrices riesgo del sistema de administración de riesgos asociados al tratamiento de datos personales.

En virtud de lo antes expuesto, los registros documentales deberán incluir como mínimo lo siguiente:

1. Una descripción genérica de las circunstancias que rodearon al incidente de seguridad, prestando especial atención a la base de datos y la clase del dato comprometido.
2. La enunciación de la categoría de los titulares de la información afectada.
3. La fecha y hora del incidente de seguridad.
4. La fecha y hora del momento en que se descubrió el incidente de seguridad.
5. Una descripción genérica de cualquier indagación o investigación que haya realizado la entidad en virtud del incidente de seguridad.

4. The procedure for handling queries and concerns that may be presented by the owners of the information.
5. The manner in which security incident reporting shall be carried out in the event of sub-contracts by the data processor shall be established.
6. The express obligation to comply with the information processing policies.

19.4.4. Preservation of internal records.

Givaudan Colombia S.A.S. shall keep documentary support, regardless of the format, whether virtual or physical, of all aspects of each security incident that occurs, in order to demonstrate compliance with the personal data protection regime in case of the opening of any administrative investigation for such reason, while such records will be used for the purpose of creating risk matrices of the risk management system associated with the processing of personal data.

By virtue of the foregoing, the documentary records shall include at least the following:

1. A generic description of the circumstances surrounding the security incident, paying particular attention to the database and the type of data compromised.
2. The enunciation of the category of the affected information holders.
3. The date and time of the security incident.
4. The date and time of the moment of discovery of the security incident.
5. A generic description of any inquiry or investigation the entity has conducted pursuant to the security incident.

6. Descripción genérica de las medidas correctivas que haya tomado la entidad en cada incidente de seguridad.
7. Datos de los responsables del manejo de cada incidente de seguridad.
8. La prueba de la notificación realizada a la Superintendencia de Industria y Comercio.
9. En caso de presentarse el incidente en medio de la ejecución de un contrato de encargatura de datos, la prueba de la notificación realizada por encargado al responsable del tratamiento de datos.
10. La prueba de la notificación del incidente al titular de la información, en caso de haber sido necesario.
11. La evaluación del nivel de riesgo derivado del incidente de seguridad en los titulares, discriminando detalladamente todos los factores tenidos en cuenta.
12. En caso de que deban establecerse, deberán incluir detalles personales del incidente de seguridad.

La entidad se compromete a:

- Documentar los incidentes de seguridad detalla y juiciosamente a fin de contar con un suficiente acervo probatorio en el escenario de una investigación o indagación por parte de la autoridad.
- Conservar el soporte documental bajo el estricto cumplimiento de las medidas de seguridad y confidencialidad necesarias para protegerla de cualquier amenaza.
- Honrar los plazos de conservación establecidos por cada organización, de acuerdo a los principios de finalidad, necesidad y proporcionalidad.
- Garantizar la originalidad e integridad de la prueba técnica en los términos de la ley 527 de 1999.

19.4.5. Protocolo de respuesta en el manejo de incidentes de seguridad.

Con fundamento en el principio de responsabilidad demostrada se establece que el Programa Integral de Gestión

6. Generic description of the corrective actions taken by the entity for each security incident.
7. Details of those controller for handling each security incident.
8. Proof of the notification made to the Superintendence of Industry and Commerce.
9. In case the incident occurs in the middle of the execution of a data entrustment contract, the proof of the notification made by the processor to the controller for the data processing.
10. The proof of the notification of the incident to the holder of the information, in case it was necessary.
11. The assessment of the level of risk derived from the security incident on the data subjects, discriminating in detail all the factors taken into account.
12. If they are to be established, they shall include personal details of the security incident.

The entity is committed to:

- Documenting security incidents in detail and judiciously in order to have sufficient evidence in the scenario of an investigation or inquiry by the authority.
- Keep the documentary support under strict compliance with the necessary security and confidentiality measures to protect it from any threat.
- Honor the retention periods established by each organization, in accordance with the principles of purpose, necessity and proportionality.
- Guarantee the originality and integrity of the technical evidence under the terms of Law 527 of 1999.

19.4.5. Security Incident Response Protocol

Based on the principle of proven responsibility, it is established that the Integral Personal Data Management Program must involve a risk management

de Datos Personales debe involucrar un componente de gestión riesgos que le permita a **Givaudan Colombia S.A.S.** identificar sus vulnerabilidades a tiempo y enfocar sus recursos en la toma de medidas de mitigación de los riesgos para todas las partes intervinientes, sea ella misma o para los titulares.

Por lo anterior, se debe contar con el protocolo de respuesta que le facilitará a **Givaudan Colombia S.A.S.** actuar de forma ordenada, eficaz y ágil ante cualquier incidente de seguridad que pueda afectar la confidencialidad, disponibilidad e integridad de los datos personales objeto de su tratamiento.

De esta manera, para efectos de esta política, se entenderá como incidente a cualquier anomalía que afecte o pudiera afectar la seguridad de las bases de datos o información contenida en las mismas.

Dado el caso de que cualquiera de los funcionarios de **Givaudan Colombia S.A.S.** llegue a conocer alguna incidencia ocurrida, debe comunicarla al Oficial de Protección de Datos, quien será el encargado de tomar las medidas oportunas frente al incidente reportado.

El Oficial de Protección de Datos informará sobre la ocurrencia de la incidencia a la Delegatura de Protección de Datos Personales de la Superintendencia de Industria y Comercio dentro de los 15 días hábiles siguientes a partir del conocimiento de esta.

Las incidencias podrán afectar tanto a las bases de datos digitales como físicas y generarán el despliegue del siguiente protocolo:

A. Notificación de incidentes

Cuando se configuren hechos que permitan intuir la ocurrencia de un incidente que pueda afectar o ver afectado las bases de datos con información personal datos personales

component that allows **Givaudan Colombia S.A.S.** to identify its vulnerabilities in time and focus its resources on taking measures to mitigate risks for all parties involved, be it itself or for the data holders.

Therefore, a response protocol must be in place that will allow **Givaudan Colombia S.A.S.** to act in an orderly, effective and agile manner in the event of any security incident that may affect the confidentiality, availability and integrity of the personal data being processed.

Thus, for the purposes of this policy, an incident shall be understood as any anomaly that affects or could affect the security of the databases or information contained therein.

In the event that any of the employees of **Givaudan Colombia S.A.S.** becomes aware of any incident that has occurred, they must communicate it to the Data Protection Officer, who will be responsible for taking the appropriate measures to deal with the reported incident.

The Data Protection Officer shall report the occurrence of the incident to the Personal Data Protection Office of the Superintendence of Industry and Commerce within 15 working days of becoming aware of it.

Incidents may affect both digital and physical databases and will generate the deployment of the following protocol:

A. Notification of incidents

When facts are configured that make it possible to intuit the occurrence of an incident that may affect or affect the databases with personal information, the Personal Data Protection Officer must be immediately

se deberá informar inmediatamente al Oficial de Protección de Datos Personales quien gestionará su reporte en el Registro Nacional de Bases de Datos.

B. Gestión de incidentes

Cada colaborador de **Givaudan Colombia S.A.S.**, ya sea trabajador, contratista, consultor o tercero, se encuentra en la obligación de reportar de manera oportuna cualquier evento sospechoso, debilidad o violación de políticas que pueden afectar la confidencialidad, integridad y disponibilidad de los activos e información personal de la entidad.

C. Identificación

Cualquier evento sospechoso o anormal, tal como aquel en el que se observe potencialmente la posibilidad de configurarse alguna pérdida de reserva o confidencialidad de la información, deberá ser evaluado para determinar si es o no, un incidente, al tiempo que, deberá ser reportado al nivel jerárquico adecuado de **Givaudan Colombia S.A.S.**

Toda determinación que incumba o involucre a las autoridades de investigación y/o judiciales debe ser hecha en conjunto entre el Oficial de Protección de Datos Personales y los asesores jurídicos de **Givaudan Colombia S.A.S.**, de igual manera, cualquier comunicación frente a dichas autoridades será realizada en conjunto por estas personas.

D. Reporte

Cualquier incidente y evento sospechoso que se presente al interior de la entidad, deberá ser reportado tan pronto como sea posible a través de los siguientes canales de comunicación que corresponden al Oficial de Protección de Datos Personales:

Correo electrónico:
francisco.alarcon@givaudan.com
Teléfono: 4252936

informed, who will manage the report in the National Registry of Databases.

B. Incident Management

Each employee of **Givaudan Colombia S.A.S.**, whether employee, contractor, consultant or third party, is obliged to report in a timely manner any suspicious event, weakness or violation of policies that may affect the confidentiality, integrity and availability of the assets and personal information of the entity.

C. Identification

Any suspicious or abnormal event, such as one in which the possibility of a loss of confidentiality of information is potentially observed, must be evaluated to determine whether or not it is an incident, and it must be reported to the appropriate hierarchical level of **Givaudan Colombia S.A.S.**

Any determination that concerns or involves investigative and/or judicial authorities must be made jointly between the Personal Data Protection Officer and the legal advisors of **Givaudan Colombia S.A.S.**, likewise, any communication with such authorities will be made jointly by these persons.

D. Report

Any incident and suspicious event that occurs within the entity must be reported as soon as possible through the following communication channels that correspond to the Personal Data Protection Officer:

Email: francisco.alarcon@givaudan.com
Phone: 4252935

En caso de que, la información sensible o confidencial se pierda, sea divulgada a personal no autorizado o se sospeche de alguno de estos eventos, el Oficial de Protección de Datos Personales, debe ser notificado de forma inmediata.

Cada uno de los funcionarios de **Givaudan Colombia S.A.S.** deberán reportar a su jefe directo y al Oficial de Protección de Datos Personales, a través de los correos electrónicos de estos, cualquier daño o pérdida de computadores o cualquier otro dispositivo, cuando estos contengan datos personales en poder de la compañía.

Ningún funcionario debe divulgar información sobre sistemas de cómputo y redes que hayan sido afectadas por un delito informático o abuso de sistema sin que alguna autoridad competente, realice la solicitud debidamente fundamentada, razonada y justificada.

Para la entrega de información o datos en virtud de orden o solicitud de autoridad competente, perentoriamente deberán intervenir, tanto el Oficial de Protección de Datos Personales como los Asesores Jurídicos de **Givaudan Colombia S.A.S.**, a fin de prestar el asesoramiento adecuado y mitigar el riesgo sancionatorio.

E. Contención, investigación y diagnóstico

El Oficial de Protección de Datos Personales, es la persona encargada de garantizar que se tomen las acciones para investigar y diagnosticar las causas que generaron el incidente, así como también debe garantizar que todo el proceso de gestión del incidente sea debidamente documentado, apoyado por la dependencia encargada del soporte tecnológico de **Givaudan Colombia S.A.S.**

Dado el caso de que se identifique algún delito informático, en los términos establecidos en la ley 1273 de 2009, será el Oficial de Protección de Datos Personales y los Asesores Jurídicos de **Givaudan Colombia S.A.S.**, los encargados de

In the event that sensitive or confidential information is lost, disclosed to unauthorized personnel, or any of these events are suspected, the Personal Data Protection Officer must be notified immediately.

Each of the employees of **Givaudan Colombia S.A.S.** must report to their direct supervisor and to the Personal Data Protection Officer, through their e-mail addresses, any damage or loss of computers or any other device, when these contain personal data held by the company.

No employee shall disclose information about computer systems and networks that have been affected by a computer crime or system abuse without a duly substantiated, reasoned and justified request from a competent authority.

For the delivery of information or data by virtue of an order or request from a competent authority, both the Personal Data Protection Officer and the Legal Advisors of **Givaudan Colombia S.A.S.** must intervene peremptorily, in order to provide the appropriate advice and mitigate the risk of sanctions.

E. Containment, investigation and diagnosis

The Personal Data Protection Officer is the person in charge of ensuring that actions are taken to investigate and diagnose the causes that generated the incident, as well as ensuring that the entire incident management process is properly documented, supported by the unit responsible for technological support **Givaudan Colombia S.A.S.**

reportar tal información a las autoridades de investigaciones judiciales competentes.

Durante toda la ejecución de los procesos de investigación, deberá garantizarse la "Cadena de Custodia" de todo el material probatorio allegado al expediente, con la finalidad de preservarlo en caso de requerirse establecer una acción legal.

F. Solución

La dependencia encargada del soporte tecnológico de **Givaudan Colombia S.A.S.**, al igual que cualquier área comprometida y los directamente responsables de la gestión de datos personales, tienen la obligación de prevenir que el incidente de seguridad se vuelva a presentar, corrigiendo todas las vulnerabilidades detectadas en la investigación interna.

G. Cierre de incidente y seguimiento

La dependencia encargada del soporte tecnológico, junto con el Oficial de Protección de Datos Personales de **Givaudan Colombia S.A.S.** y las demás dependencias o áreas que usan o requieren la información, deberán desplegar actividades de documentación y revisión de las acciones que fueron ejecutadas para remediar el incidente de seguridad.

El Oficial de Protección de Datos Personales preparará un análisis anual de los incidentes reportados. Las conclusiones de este informe se utilizarán en la elaboración de campañas de concientización que ayuden a minimizar la probabilidad de incidentes futuros.

In the event that a computer crime is identified, under the terms established in Law 1273 of 2009, the Personal Data Protection Officer and the Legal Advisors of **Givaudan Colombia S.A.S.**, will be responsible for reporting such information to the competent judicial investigation authorities.

Throughout the execution of the investigation process, the "Chain of Custody" of all evidentiary material submitted to the file must be guaranteed in order to preserve it in case legal action is required.

F. Solution

The unit in charge of the technological support of **Givaudan Colombia S.A.S.**, as well as any compromised area and those directly responsible for the management of personal data, have the obligation to prevent the security incident from happening again, correcting all the vulnerabilities detected in the internal investigation.

G. Incident closure and follow-up

The unit in charge of technological support, together with the Personal Data Protection Officer of **Givaudan Colombia S.A.S.** and the other units or areas that use or require the information, shall deploy activities of documentation and review of the actions that were executed to remedy the security incident.

The Personal Data Protection Officer shall prepare an annual analysis of the reported incidents. The findings of this report will be used in the development of awareness campaigns to help minimize the likelihood of future incidents.

H. Reporte de incidente ante la SIC como autoridad de control

Serán reportados como novedades los incidentes de seguridad que afecten las bases de datos de acuerdo con las siguientes reglas:

Cualquier violación de los códigos de seguridad o la pérdida, robo y/o acceso no autorizado de información de una base de datos administrada por el Responsable del Tratamiento o por su Encargado, deberán reportarse al Registro Nacional de bases de Datos dentro de los quince (15) días hábiles siguientes al momento en que se detecte y sea puesta en conocimiento de la persona o área encargada de atenderlos.

Todos los líderes de cada proceso y/o propietarios de activos de información de **Givaudan Colombia S.A.S.**, reportarán de forma interna los incidentes de seguridad relacionados a datos personales ante el Oficial de Protección de Datos Personales, quien dentro del plazo legal procederá a reportarlos ante el Registro Nacional de Bases de Datos.

H. Incident report to the SIC as a control authority.

Security incidents affecting the databases shall be reported as new developments in accordance with the following rules:

Any violation of the security codes or the loss, theft and/or unauthorized access of information from a database managed by the Data Controller or its Processor, shall be reported to the National Registry of databases within fifteen (15) working days from the time it is detected and brought to the attention of the person or area in charge of dealing with them.

All the leaders of each process and/or owners of information assets of **Givaudan Colombia S.A.S.**, will report internally the security incidents related to personal data to the Personal Data Protection Officer, who within the legal term will proceed to report them to the National Registry of Databases.

19.5. Políticas y procedimientos orientado a atención de PQR	19.5. Policies and procedures oriented to PQR attention
---	--

19.5.1. Introducción	19.5.1. Introduction
-----------------------------	-----------------------------

Este manual tiene como propósito establecer los lineamientos y parámetros generales para el mejoramiento de los procesos internos requeridos para la atención de:

- Peticiones
- Quejas
- Reclamos
- Solicitudes
- Sugerencias

En adelante llamados “PQR”, presentados por los titulares de información personal que sean tratados por “Givaudan ”, y que sean presentados a través de los canales autorizados por la compañía.

Givaudan Colombia SAS adhiere a esta política, a su vez, de manera integral las siguientes políticas globales de tratamiento de datos personales:

- Data Subject Rights Requests Policy
- Global Privacy and Data Protection Policy
- Global Employees and Contractors Privacy Notice
- Global Picture and Video Management Policy
- Personal data Protection Guidelines for Marketing and Communication teams.
- Personal Data Breach Handling Policy and Procedure
- IM&T Security Policies

De igual forma pretende optimizar los procesos internos para disminuir los riesgos de imposición de multas administrativas por parte de la Superintendencia de Industria y Comercio que versen sobre servicios e información y en general todas las normas que enmarcan la protección al consumidor.

The purpose of this manual is to establish the general guidelines and parameters for the improvement of the internal processes required to attend to the needs of clients:

- Petitions
- Complaints
- Claims
- Requests
- Suggestions

Hereinafter referred to as "PQR", submitted by the holders of personal information that are processed by "Givaudan ", and that are submitted through the channels authorized by the company.

Givaudan Colombia SAS adheres to this policy, in turn, in a comprehensive manner, the following global personal data processing policies:

- Data Subject Rights Requests Policy
- Global Privacy and Data Protection Policy
- Global Employees and Contractors Privacy Notice
- Global Picture and Video Management Policy
- Personal data Protection Guidelines for Marketing and Communication teams.
- Personal Data Breach Handling Policy and Procedure.
- IM&T Security Policies

It also pretend to optimize internal processes to reduce the risk of administrative fines imposed by the Superintendence of Industry and Commerce regarding

Es interés de la compañía velar por el cumplimiento de los deberes y el reconocimiento de los derechos de los usuarios en condiciones de calidad y oportunidad de acuerdo a los principios y valores institucionales, poniendo en conocimiento interno el siguiente manual de atención, al derecho que le asiste a las contrapartes de Givaudan para presentar solicitudes y obtener respuestas de manera oportuna y eficiente, en cumplimiento de las normas establecidas en el ordenamiento jurídico colombiano, especialmente en la Ley 1581 de 2012 y demás normas que lo complementen, reglamenten y /o modifiquen.

19.5.2. Alcance

El presente manual aplicará para la compañía en todas sus áreas disponibles en la operación nacional. A través del correo electrónico, Email: francisco.alarcon@givaudan.com

se atenderán las peticiones, quejas, reclamos, solicitudes y sugerencias con la oportunidad que exigen la Constitución y las leyes.

El objetivo de Givaudan Colombia S.A.S., en adelante "GIVAUDAN", es atender y solucionar oportunamente las necesidades de los titulares de información personal cuyo tratamiento esté en cabeza de la compañía Titular de la información personal, de esta manera obtener altos niveles de satisfacción y de cumplimiento del ordenamiento jurídico vigente. Para ello divulgamos el presente manual a nuestros funcionarios y los capacitamos continuamente.

Para todos los requerimientos de atención de PQR que ingresen directamente al correo electrónico francisco.alarcon@givaudan.com o lleguen trasladados al mismo por el Oficial de privacidad ó cualquier ente de vigilancia, el "OP" cuenta con un tiempo máximo de quince (15) días hábiles después de realizada la radicación para dar respuesta al Titular de la información personal, la cual debe

services and information and, in general, all the rules that frame consumer protection.

It's in the interest of the company to ensure compliance with the duties and recognition of the rights of users in conditions of quality and timeliness in accordance with the principles and institutional values, making internal knowledge the following service manual, to the right that have of Givaudan 's counterparties to submit requests and obtain answers in a timely and efficient manner, in compliance with the rules established in the Colombian legal system, especially in Law 1581 of 2012 and other rules that complement, regulate and / or modify it.

19.5.2. Scope

This manual shall apply to the company in all areas available in the national operation. Through e-mail Francisco.alarcon@givaudan.com requests, complaints, claims, requests and suggestions will be addressed with the timeliness required by the Constitution and laws.

The objective of Givaudan Colombia S.A.S., hereinafter "GIVAUDAN ", is to attend and solve in a timely manner the needs of the holders of personal information whose treatment is in the hands of the company that holds the personal information, thus obtaining high levels of satisfaction and compliance with current legislation. To this end, we disseminate this manual to our employees and train them continuously.

For all requests for attention of PQR that enter directly to the email Francisco.alarcon@givaudan.com or are transferred to it by the Privacy Officer or any oversight

ser remitida a la última dirección de correspondencia física o virtual que se tenga del Titular de la información personal.

19.5.3. Políticas y controles a nivel de atención de los titulares de la información personal

A continuación, se indican las políticas que orientan la gestión y atención de los PQR presentadas por los Titulares de la información personal a través de los diferentes canales, bajo estas políticas se ejercerá control de cara a buscar su cumplimiento y satisfacción del Titular de la información personal.

Este proceso estará sujeto a control de indicadores señalados también dentro del presente numeral.

a) Política 1:

Todo Titular de la información personal que sea manejada por Givaudan recibirá por parte de la compañía, atención a través de correo electrónico francisco.alarcon@givaudan.com, en la cual el asesor le dará solución a las solicitudes o inconformidades planteadas por este.

Control: ¿Cuál es el control establecido para el cumplimiento de esta política? Indicador: Indicador de satisfacción del Titular de la información personal en el aspecto evaluado.

b) Política 2:

El Titular de la información personal recibirá por parte de nuestros colaboradores, respuesta y solución oportuna a preguntas y dudas con el fin de generar un ambiente de atención, protección y respeto bajo un concepto de servicio de calidad, claridad en la recepción de requerimientos, enfoque comercial y de estricto cumplimiento del ordenamiento jurídico.

body, the "PO" has a maximum of fifteen (15) working days after the filing to respond to the Holder of the personal information, which must be sent to the last physical or virtual correspondence address of the Holder of the personal information.

19.5.3. Policies and controls at the level of attention of the holders of personal information

The following are the policies that guide the management and attention of the PQR submitted by the Holders of personal information through the different channels, under these policies control will be exercised in order to seek compliance and satisfaction of the Holder of personal information.

This process will be subject to control of indicators also indicated in this numeral.

a) Policy 1:

Any holder of personal information handled by Givaudan will receive attention from the company through the the email francisco.alarcon@givaudan.com, in which the advisor will provide a solution to the requests or disagreements raised by the holder.

Control: What is the control established for compliance with this policy? Indicator: Indicator of satisfaction of the holder of the personal information in the evaluated aspect.

b) Policy 2:

The holder of personal information will receive from our employees, response and timely solution to questions and doubts in order to generate an atmosphere of care, protection and respect under a concept of quality service, clarity in receiving

Control: Indicador de satisfacción del Titular de la información personal en el aspecto evaluado. Formulario de evaluación de la requisición diligenciado por quién la hizo.

c) Política 3:

“GIVAUDAN” entregará al Titular de la información personal información transparente, suficiente, cierta, clara y oportuna sobre la información que es tratada por la compañía en su calidad de responsable y sobre las PQR presentadas por estos, aplicando la debida diligencia exigida por los entes de control frente a las respuestas de los PQR.

Control: ¿Cuál es el control a implementar o implementado?

Indicador: Indicador de satisfacción del Titular de la información personal – Indicador de tiempos de respuesta a PQR.

d) Política 4:

Las PQR presentadas por el Titular de la información personal, se atenderán de forma clara, completa y eficaz (calidad de la respuesta), orientándose a ofrecer una solución definitiva o de fondo a los Titular de la información personal, siempre que ello sea posible y procedente conforme lo dispone la normatividad vigente.

Control: Indicador: Indicador de calidad de respuesta de PQR.

e) Política 5:

“GIVAUDAN” ofrecerá a todo Titular de la información personal una respetuosa atención desde el momento previo a la autorización del tratamiento de la información personal con la compañía, buscando de manera permanente y proactiva evitar que se presenten PQR por factores atribuibles a actitudes inadecuadas del personal de la compañía.

requirements, commercial approach and strict compliance with the law.

Control: Indicator of satisfaction of the holder of personal information in the evaluative aspect. An assessment form must be filled by the person who open the request

c) Policy 3:

"GIVAUDAN " will deliver to the Holder of the personal information transparent, sufficient, certain, clear and timely information about the information that is processed by the company in its capacity as responsible and about the PQR submitted by them, applying the due diligence required by the control entities regarding the answers to the PQR.

Control: Indicator of satisfaction of the holder of personal information - Indicator of response times to PQR.

d) Policy 4:

The PQR submitted by the Holder of the personal information shall be handled in a clear, complete and effective manner (quality of the response), aiming to offer a definitive or substantive solution to the Holder of the personal information, whenever possible and appropriate, in accordance with the provisions of the regulations in force.

Control: Indicator: PQR response quality indicator.

e) Policy 5:

"GIVAUDAN " will offer to every Personal Information Holder a respectful attention from the moment prior to the authorization of the processing of personal information with the company, permanently and proactively seeking to avoid the occurrence of

Control: Indicador de satisfacción de los Titular de la información personal e indicador de quejas por calidad de la atención.

f) Política 6:

Los colaboradores de Givaudan conocerán de manera clara y completa las políticas, funciones y procedimientos internos en la gestión y atención de PQR a través de programas de capacitación y formación interna, que estarán a cargo del "OP", los cuales involucran temas de atención, asesoría, autonomía en el ofrecimiento de soluciones, amabilidad, empatía, y gestión de los PQR presentados por los Titular de la información personal.

Control: Se deberá dar a conocer a todo el personal de la Compañía sin excepción todo el contenido del presente Manual y procedimientos asociados. Se realizarán encuestas aleatorias automáticas a los Titular de la información personal que solicitan la gestión del personal de atención al Titular de la información personal en el punto de atención.

Indicador: Indicador de asistencia a la capacitación del Manual, Indicador de entendimiento/ dominio de conocimientos, Indicador de evaluaciones aleatorias al personal de la Compañía que sean realizadas por el "OP".

g) Política 7:

La Compañía propenderá por dar a conocer los deberes, derechos, y canales de comunicación con que el Titular de la información personal cuenta para la presentación de sus quejas y reclamos, cumpliendo así con el deber de comunicación a y de acceso a la información personal que será tratada por Givaudan como responsable.

Control: Bitácora de publicación de información mediante material impreso o electrónico en el que se enviará información o tips informativos al Titular de la información

PQR due to factors attributable to inadequate attitudes of the company's personnel.

Control: Indicator: Personal information holder satisfaction indicator and quality of care complaints indicator.

f) Policy 6:

Givaudan 's employees will know clearly and completely the policies, functions and internal procedures in the management and care of PQR through training programs and internal training, which will be in charge of the "PO", which involve issues of care, advice, autonomy in providing solutions, kindness, empathy, and management of PQR submitted by the holders of personal information.

Control: All Company personnel, without exception, shall be made aware of the contents of this Manual and associated procedures. Automatic random surveys shall be carried out to the Personal Information Holders who request the management of the Personal Information Holder service personnel in the point of focus.

Indicator: Indicator of attendance to the Manual training, Indicator of understanding / mastery of knowledge, Indicator of random evaluations of the Company's personnel carried out by the "OP".

g) Policy 7:

The Company'll endeavor to make known the duties, rights and communication channels available to the Holder of personal information for the submission of complaints and claims, thus complying with the duty of communication and access to personal information that will be treated by Givaudan as the responsible party.

personal que labore en la Compañía, información que permita a su vez la actualización del presente Manual. Medición de satisfacción del Titular de la información personal en el punto específico en que se identifique si el Titular de la información personal conoce la información ofrecida por la Compañía.

Indicador: Indicador de Satisfacción del Titular de la información personal. Indicador cantidad de novedades en información / cantidad de novedades informadas.

Informe Mensual: Mensualmente se elaborará por el Oficial de privacidad un informe detallado de cada una de las quejas y reclamos recibidos.

Fecha de Queja y/o Reclamo • Queja y/o Reclamo presentado • Trazabilidad de la Queja y/o Reclamo • Solución de la Queja y/o Reclamo. • Fecha de cierre de Queja y/o Reclamo

19.5.4. Procedimientos a nivel de atención de pqr de los titulares de la información personal

19.5.4.1. Generalidades

El Titular de la información personal podrá presentar Peticiones, Quejas, Reclamos, Recursos o Solicitudes (PQR) en forma verbal o escrita, para lo cual no requerirá presentación personal ni intervención de abogado, aunque el Titular de la información personal autorice a otra persona para que presente una PQR, y mediante los medios tecnológicos o electrónicos asociados a los mecanismos de atención al Titular de la información personal que las oficinas virtuales y la línea telefónica Por su parte, "GIVAUDAN " tiene la obligación de recibir, atender, tramitar y responder las PQR que presente el Titular de la información personal.

Para responder una PQR, "GIVAUDAN" cuenta con un término de quince (15) días hábiles contados a partir del día siguiente a la fecha de su presentación, salvo que se trate de petición de documentos, caso en el cual "GIVAUDAN" deberá resolverla dentro de los diez (10) días siguientes a su

Control: Information publication log by means of printed or electronic material in which information or informative tips will be sent to the Holder of the personal information working in the Company, information that in turn allows the updating of this Manual. Measurement of satisfaction of the Holder of the personal information in the specific point in which it is identified if the Holder of the personal information is aware of the information offered by the Company.

Indicator: Personal Information Holder Satisfaction Indicator. Indicator number of new information / number of new information reported.

Monthly Report: On a monthly basis, the Privacy Officer will prepare a detailed report of each of the complaints and claims received.

Date of Complaint and/or Claim - Complaint and/or Claim filed - Traceability of the Complaint and/or Claim - Solution of the Complaint and/or Claim. - Date of closure of Complaint and/or Grievance

19.5.4. Procedures at the level of attention of pqr of the holders of personal information

19.5.4.1. Generalities

The Holder of the personal information may submit Petitions, Complaints, Claims, Appeals or Requests (PQR) verbally or in writing, for which no personal presentation or intervention of a lawyer shall be required, even if the Holder of the personal information authorizes another person to submit a PQR, and through the technological or electronic means associated with the mechanisms of attention to the Holder of the personal information that the virtual offices and the telephone line For its part, "GIVAUDAN " has the obligation to receive, attend,

recepción. Este término se podrá ampliar para la práctica de pruebas, en un término no mayor a 15 días prorrogables por una sola vez sin que con la prórroga el término exceda de 15 días, en caso de ser necesarias, previa motivación y comunicación de esta situación al Titular de la información personal. En caso que "GIVAUDAN" constate que una petición ya radicada está incompleta, pero la actuación puede continuar sin oponerse a la ley, requerirá al peticionario dentro de los diez (10) días siguientes a la fecha de radicación para que la complete en el término máximo de un (1) mes; a partir del día siguiente en que el Titular de la información personal aporte los documentos o informes requeridos, comenzará a correr el término para resolver la petición.

Ahora bien, para los Reclamos por protección de datos personales, "GIVAUDAN" cuenta con un término de quince (15) días hábiles contados a partir del día siguiente a su recibo, este término se podrá ampliar en un término no mayor a 8 días hábiles, en este caso se informará al interesado los motivos de la demora y la fecha en que se atenderá su reclamo. Si el reclamo resulta incompleto, se requerirá al interesado dentro de los 5 días siguientes a la recepción del reclamo para que subsane las fallas.

Transcurridos dos (2) meses desde la fecha de presentación del requerimiento sin que el solicitante presente la información requerida, se entenderá que ha desistido tácitamente del requerimiento, por lo que se procederá a su archivo.

Cuando se presente una PQR de forma verbal, basta con que el Titular de la información personal informe el nombre completo, número de identificación y el motivo de la solicitud; en caso de que una PQR se presente de forma escrita, adicionalmente a los requisitos indicados, deberá contener la dirección de notificación. "GIVAUDAN".

La decisión de las peticiones, quejas, reclamos deberán ser remitidas por GIVAUDAN COLOMBIA S.A.S. a la dirección de notificación reportada por el Titular de la información personal. cuando "GIVAUDAN" realice

process and respond to the PQR submitted by the Holder of the personal information.

To respond to a PQR, "GIVAUDAN " has a term of fifteen (15) working days from the day following the date of its submission, unless it is a request for documents, in which case "GIVAUDAN " must resolve it within ten (10) days from its receipt. This term may be extended for the practice of evidence, in a term not exceeding 15 days, extendable only once without the extension of the term exceeding 15 days, if necessary, prior motivation and communication of this situation to the Holder of the personal information. In case "GIVAUDAN " finds that a petition already filed is incomplete, but the action can continue without opposing the law, it will require the petitioner within ten (10) days from the date of filing to complete it within a maximum term of one (1) month; from the next day in which the Holder of the personal information provides the required documents or reports, the term to resolve the petition will begin to run.

Now, for claims for the protection of personal data, "GIVAUDAN " has a term of fifteen (15) working days from the day following its receipt, this term may be extended in a period not exceeding 8 working days, in this case the person concerned will be informed of the reasons for the delay and the date on which the claim will be addressed. If the claim is incomplete, the interested party will be required within 5 days of receipt of the claim to correct the faults.

After two (2) months from the date of submission of the request without the applicant submitting the required information, it will be understood that the request has been tacitly withdrawn, so it will be filed.

When a PQR is submitted verbally, it is sufficient for the Holder of the personal information to inform the

notificaciones electrónicas al correo del Titular de la información personal, respecto de las decisiones de una PQR.

Así mismo, "GIVAUDAN" podrá implementar mecanismos alternos de notificación en línea a través de internet, en los cuales el Titular de la información personal pueda acceder al contenido de la decisión empresarial mediante la asignación previa de un Titular de la información personal y clave de acceso.

19.5.4.2. Procedimiento de atención a Requerimientos

El proceso de atención a requerimientos se dividirá en cinco etapas:

- **Recepción de PQR:** Es la etapa en la que se reciben y registran los Requerimientos a través de los diferentes canales dispuestos por "GIVAUDAN".
- **Gestión de PQR:** Es la etapa en la que se investiga lo relacionado al requerimiento, se realizan los ajustes respectivos y se genera una solución o respuesta.
- **Respuesta de PQR:** Es la etapa en la que se le informa el resultado del requerimiento.
- **Medición de PQR:** Es la etapa en la que se generan estadísticas respecto de las diferentes tipologías de quejas o reclamos para su análisis y determinación de planes de mejora.
- **Calidad de PQR:** Es la etapa en la que se generan estadísticas respecto de la calidad aplicada a los procesos de quejas o reclamos.

19.5.4.3. Recepción de PQR

full name, identification number and the reason for the request; in the event that a PQR is submitted in writing, in addition to the requirements indicated, it must contain the notification address. "GIVAUDAN".

The decision of the petitions, complaints, claims shall be sent by GIVAUDAN COLOMBIA S.A.S. to the notification address reported by the Holder of the personal information. when "GIVAUDAN" makes electronic notifications to the email of the Holder of the personal information, regarding the decisions of a PQR.

Likewise, "GIVAUDAN" may implement alternative online notification mechanisms through the Internet, in which the Holder of the personal information may access the content of the corporate decision by previously assigning a Holder of the personal information and password.

19.5.4.2. Procedure for attending to Requests

The process of attending to requirements will be divided into five stages:

- **PQR Reception:** This is the stage in which the Requests are received and registered through the different channels provided by "GIVAUDAN".
- **PQR Management:** It is the stage in which the requirement is investigated, the respective adjustments are made and a solution or response is generated.
- **PQR Response:** It is the stage in which you are informed of the result of the requirement.
- **PQR Measurement:** It is the stage in which statistics are generated regarding the different types of complaints or claims for analysis and determination of improvement plans.

Los funcionarios de la Compañía quienes reciben los reclamos, quejas y solicitudes de información proceden a radicar el requerimiento en (SISTEMA QUE GIVAUDAN DESIGNE PARA EL TRATAMIENTO DE LAS PQR'S). Radicado el requerimiento se deberá proceder a informar el número de radicado, evaluar si pueden solucionar el requerimiento del Titular de la información personal de manera inmediata o de lo contrario le comunican la fecha estimada de solución y, en caso de ser necesario, solicitan documentación soporte.

Toda la documentación que soporte el reclamo debe remitirse a la dirección de correo electrónico descrita posteriormente al interior de este capítulo.

Los requerimientos pueden ingresar por cualquiera de los canales de atención que tiene disponibles "GIVAUDAN" para este fin:

- Email: francisco.alarcon@givaudan.com
- **Requerimientos Escritos:** Son las solicitudes que llegan vía carta a las oficinas de "GIVAUDAN" directamente de los Titulares de la información personal, que son radicados ante la SIC y de los entes legales como la Fiscalía, Policía, Contraloría y Ministerio de Defensa, entre otros.

Así mismo, es necesario tener en cuenta que estos medios de atención, deben cumplir con los siguientes requisitos:

1. El Titular de la información personal puede acceder de manera gratuita a cualquier medio de atención, en cualquier momento, salvo las líneas telefónicas.
2. Todos los trámites deben ser sencillos,
3. En las solicitudes que requieran la verificación de identidad del Titular de la información personal, la misma deberá adelantarse por "GIVAUDAN", a través de mecanismos confiables de validación.

• **Quality of PQR:** This is the stage in which statistics are generated regarding the quality applied to complaints or claims processes.

19.5.4.3. PQR Reception

Company officials who receive claims, complaints and requests for information proceed to file the request in (SYSTEM DESIGNATED BY GIVAUDAN FOR THE PROCESSING OF PQR'S). Once the request has been filed, they shall proceed to inform the filing number, evaluate if they can solve the requirement of the Holder of the personal information immediately or otherwise inform the estimated date of solution and, if necessary, request supporting documentation.

All documentation supporting the claim must be sent to the e-mail address described later in this chapter.

The requirements can be entered through any of the service channels that "GIVAUDAN " has available for this purpose:

- Email: francisco.alarcon@givaudan.com
- **Written Requests:** These are the requests that arrive via letter to the offices of "GIVAUDAN " directly from the Holders of personal information, which are filed before the SIC and legal entities such as the Prosecutor's Office, Police, Comptroller's Office and Ministry of Defense, among others.

Likewise, it's necessary to take into account that these means of attention must comply with the following requirements:

1. The holder of the personal information may access free of charge to any means of attention, at any time, except for telephone lines.

4. Todo lo que sea informado al Titular de la información personal a través de cualquier medio de atención obliga y compromete a "GIVAUDAN".

De otro lado, los requerimientos presentados deberán contener como mínimo la información que se discrimina a continuación:

- a) Nombres y apellidos del titular y/o su representante y/o causahabiente.
- b) Lo de se pretende consultar.
- c) Dirección física, electrónica y teléfono de contacto del titular y/o sus causahabientes o representantes.
- d) Firma, número de identificación o procedimiento de validación que corresponda.
- e) Que se haya presentado a través de los canales dispuestos por "GIVAUDAN".

i. Descripción del proceso de recepción de los PQR

Se han de atender todas las solicitudes que ingresen por cualquiera de los canales de atención sin ningún tipo de omisión ni restricción aclarando las dudas y solicitudes de los Titulares de la información personal, haciendo las validaciones necesarias, dejando registro de las solicitudes por peticiones, incidencias o quejas en los aplicativos, informando tiempos de respuesta y número de radicado; si es posible dando solución en el primer contacto, de lo contrario escalando el caso al "OP" dejándolo en estado de análisis para que se hagan las validaciones necesarias y se comuniquen posteriormente para dar respuesta en los tiempos establecidos.

ii. Procedimientos alrededor de la recepción de los PQR

Hace parte del proceso, las validaciones de los datos y análisis de los casos, así como solicitud de soportes en los casos que sea necesario, de acuerdo con los siguientes canales de ingreso:

- 2. All procedures must be simple,
- 3. In the requests that require the verification of the identity of the Holder of the personal information, the same shall be carried out by "GIVAUDAN ", through reliable validation mechanisms.
- 4. Everything that is informed to the Holder of the personal information through any means of attention obliges and commits "GIVAUDAN"

On the other hand, the requests submitted must contain at least the following information:

- a) Names and surnames of the holder and/or its representative and/or assignee.
- b) The information to be consulted.
- c) Physical and electronic address and contact telephone number of the holder and/or its assignees or representatives.
- d) Signature, identification number or corresponding validation procedure.
- e) That it has been submitted through the channels provided by "GIVAUDAN".

i. Description of the PQR reception process

All requests received through any of the service channels must be attended without any type of omission or restriction, clarifying the doubts and requests of the holders of personal information, making the necessary validations, leaving a record of the requests for petitions, incidents or complaints in the applications, informing response times and file number; if possible providing a solution in the first contact, otherwise escalating the case to the "PO" leaving it in analysis status so that the necessary validations are made and then communicate to respond within the established timeframes.

ii. Procedures around the reception of PQRs

The process includes the validation of data and analysis of cases, as well as the request for support when

- Correo: francisco.alarcon@givaudan.com: Estas solicitudes o soportes de las solicitudes llegan al correo del oficial de privacidad para ser gestionadas en los tiempos establecidos.
- Entes Legales: estas solicitudes pueden llegar por medio físico o virtual, se registra el caso en el (SISTEMA QUE GIVAUDAN DESIGNE PARA EL TRATAMIENTO DE LAS PQR'S)(sistema que Givaudan designe para el tratamiento de las PQR's) en la misma fecha que se recibe, se valida si las solicitudes corresponden a Titulares de la información personal cuyo responsable sea "GIVAUDAN " registrados en (SISTEMA QUE GIVAUDAN DESIGNE PARA EL TRATAMIENTO DE LAS PQR'S), se envía respuesta por el mismo medio recibido (carta, e-mail).
- Oficial de privacidad: Son los reclamos recibidos directamente por el Oficial de privacidad, quien los remite a "GIVAUDAN " para que sean tramitados directamente por éste y/o por el área a este asignado.

iii. Funcionarios encargados

Las solicitudes serán atendidas por el oficial de privacidad cuando ingresen por el canal telefónico utilizando los protocolos establecidos; si ingresan por otro de los canales llegará directamente al "OP" para ser analizados y resueltos. Si se requiere, las solicitudes pueden ser escaladas a otras áreas a nivel de soporte para dar la solución.

necessary, in accordance with the following entry channels:

- Mail: Francisco.alarcon@givaudan.com: These requests or supports of the requests arrive to the mail of privacy officer to be managed in the established times.
- Legal Entities: these requests may arrive by physical or virtual means, the case is registered in the (SYSTEM THAT GIVAUDAN DESIGNATES FOR THE TREATMENT OF PQR'S)(system that Givaudan designates for the treatment of PQR's) on the same date it is received, validates if the requests correspond to Personal Information Holders whose controller is "GIVAUDAN " registered in (SYSTEM DESIGNATED BY GIVAUDAN FOR THE TREATMENT OF PQR'S), a response is sent by the same means received (letter, e-mail).
- Privacy Officer: Complaints received directly by the Privacy Officer, who forwards them to "GIVAUDAN " to be processed directly by him/her and/or by the area assigned to him/her.

iii. Officials in charge

Requests will be handled by the privacy officer when they come in through the telephone channel using the established protocols; if they come in through other channels, they will go directly to the "OP" to be analyzed and resolved. If required, requests can be escalated to other areas at the support level to provide a solution.

19.5.5. Gestión de PQR

i. Descripción del proceso de gestión de los PQR

Las solicitudes de PQR deben ser ingresadas a los aplicativos, teniendo en cuenta la razón principal de la queja, diligenciando los campos establecidos, haciendo las validaciones requeridas y dejando de manera clara las observaciones de las quejas.

ii. Procedimiento alrededor de la gestión de los PQR

QUEJAS RECIBIDAS DIRECTAMENTE EN "GIVAUDAN": El "OP" deberá registrar en el módulo de gestión, y en conjunto con el Supervisor y el Gerente de Operaciones, analizarán la tipología de la queja, para lo cual se deberá tener en cuenta las siguientes:

- Información. El Titular de la información personal señala que su información personal es incorrecta y/o no ha sido autorizada para el tratamiento
- Tratamiento. La información personal fue tratada en contravención de las autorizaciones conferidas por el titular.
- Transferencia de información. El titular de la información señala que no se ha aprobado por parte de este la transferencia de información a terceros.

Una vez validadas las tipologías, y reunida la respectiva trazabilidad del caso se determinará si se procede o no a dar favorabilidad al reclamante, directriz que deberá ser tomada una vez evaluado el material probatorio.

El área de Finanzas por intermedio del Oficial de Privacidad OP, será el responsable de analizar la queja haciendo trazabilidad al expediente, indagando sobre lo sucedido con las personas involucradas.

19.5.5. PQR Management

i. Description of the PQR management process

PQR requests must be entered into the applications, taking into account the main reason for the complaint, filling in the established fields, making the required validations and clearly stating the observations of the complaints.

ii. Procedure for PQR management

COMPLAINTS RECEIVED DIRECTLY IN "GIVAUDAN ": The "PO" shall register in the management module, and together with the Supervisor and the Operations Manager, shall analyze the typology of the complaint, for which the following shall be taken into account:

- Information. The Holder of the personal data indicates that his/her personal data are erroneous and/or have not been authorized for processing.
- Processing. The personal information was processed in contravention of the authorizations conferred by the holder.
- Transfer of information. The data holder points out that the transfer of information to third parties has not been approved by the data holder.

Once the typologies have been validated, and the respective traceability of the case has been gathered, it will be determined whether or not to proceed to give favorability to the complainant, a guideline that must be taken once the evidentiary material has been evaluated.

The Finance area, and its privacy officer will be responsible for analyzing the complaint by tracing the

Una vez ejecutados los pasos señalados se contactará al reclamante para darle respuesta formal a su reclamación si la misma fue radicada telefónicamente, si se recibió de forma escrita la misma deberá ser atendida por escrito en un término de 15 días hábiles contados a partir del día siguiente de su radicación.

Si evaluada la trazabilidad la queja del reclamante se encuentra infundada y el material probatorio demuestra que lo que dice no corresponde a la realizada se deberá emitir respuesta por el mismo canal que se recibió la petición, dicha comunicación deberá ir acompañada con llamada de venta, correo de envío términos y condiciones y demás elementos que demuestren que la compañía actuó con diligencia.

QUEJAS RECIBIDAS A TRAVES DEL OFICIAL DE PRIVACIDAD: Son las quejas que son interpuestas directamente en el Oficial de privacidad y trasladadas al Gerente General de GIVAUDAN, El Gerente General analiza toda la trazabilidad de la queja y se comunicará directamente con el Oficial de privacidad, rindiendo un informe de la queja presentada. Una vez se le haya informado al Oficial de privacidad y acuerden una solución, Gerencia General le enviará dicha solución al área de Finanzas de "GIVAUDAN" para dar cierre a esta, en un plazo máximo de 24 horas.

iii. Derechos Garantizados mediante el Procedimiento:

- a) Corrección o actualización: "GIVAUDAN" y/o cualquier encargado, garantizarán a los titulares de datos personales contenidos en sus bases de datos o a sus causahabientes, el derecho de corregir o actualizar los datos personales que reposen en sus bases de datos, mediante la presentación de la respectiva reclamación, cuando consideren que se cumplen los parámetros establecidos por la ley o los señalados en la presente política.
- b) Revocatoria de la autorización o supresión de los datos personales: "GIVAUDAN" y/o cualquier encargado,

file, inquiring about what happened with the persons involved.

Once the steps indicated above have been executed, the complainant will be contacted to give a formal response to the complaint if it was filed by telephone; if it was received in writing, it must be answered in writing within 15 working days from the day after it was filed.

If, after evaluating the traceability, the complainant's complaint is found to be unfounded and the evidentiary material demonstrates that what he/she says does not correspond to what was done, a response must be issued through the same channel that the request was received, such communication must be accompanied by a sales call, mailing of terms and conditions and other elements that demonstrate that the company acted diligently.

COMPLAINTS RECEIVED THROUGH THE PRIVACY OFFICER: These are the complaints that are filed directly with the Privacy Officer and transferred to the "PO" of "GIVAUDAN ", The General Manager analyzes all the traceability of the complaint and will communicate directly with the Privacy Officer, providing a report of the complaint filed. Once the Privacy Officer has been informed and a solution has been agreed upon, the General Manager will send the solution to the Finance area of "GIVAUDAN " to close the complaint within a maximum period of 24 hours.

iii. Rights Guaranteed through the Procedure:

- a) Correction or update: "GIVAUDAN" and/or any person in charge, will guarantee the holders of personal data contained in their databases or their successors, the right to correct or update the personal data contained in their databases, by filing the respective claim, when they consider that

garantizarán a los titulares de datos personales contenidos en sus bases de datos o a sus causahabientes, el derecho de solicitar la revocatoria de la autorización o solicitar supresión de la información contenida en su registro individual o toda aquella que esté vinculada con su identificación cuando consideren que se cumplen los parámetros establecidos por la ley o lo señalados en la presente política. De igual forma, se garantizará el derecho de presentar reclamos cuando adviertan el presunto incumplimiento de la ley 1581 de 2012 o de la presente política.

En caso de resultar procedente lo Supresión de los datos del titular de la base de datos conforme a la reclamación presentada, "GIVAUDAN" deberá realizar operativamente la supresión de tal manera que la eliminación no permita la recuperación de la información, sin embargo, el Titular deberá tener en cuenta que en algunos casos cierta información deberá permanecer en registros históricos por cumplimiento de deberes legales de la organización por lo que su supresión versará frente al tratamiento activo de los mismo y de acuerdo a la solicitud del titular.

the parameters established by law or those indicated in this policy are met.

b) Revocation of authorization or deletion of personal data: "GIVAUDAN" and/or any person in charge, shall guarantee the holders of personal data contained in its databases or their successors, the right to request the revocation of authorization or request deletion of the information contained in their individual record or any information that is linked to their identification when they consider that the parameters established by law or as indicated in this policy are met. Similarly, the right to file claims will be guaranteed when they notice the alleged breach of Law 1581 of 2012 or this policy.

In the event that the deletion of the holder's data from the database is appropriate in accordance with the claim filed, "GIVAUDAN" shall operationally perform the deletion in such a way that the deletion does not allow the recovery of the information, however, the Holder shall take into account that in some cases certain information must remain in historical records in compliance with legal duties of the organization, so that its deletion will deal with the active treatment of the same and in accordance with the request of the holder.

<p>19.6. Política general de seguridad y privacidad de la información</p>	<p>19.6. General information security and privacy policy.</p>
<p>19.6.1. Alcance</p> <p>Para “GIVAUDAN”, la protección de la información tiene como objeto, mantener un nivel de exposición, acorde con el objeto social que desarrolla, que le permita responder por la integridad, confidencialidad y la disponibilidad de esta.</p> <p>De acuerdo con lo anterior, esta política aplica a los directivos, colaboradores, proveedores, clientes y en general a cualquier persona que tenga acceso a la información tratada por “GIVAUDAN”, estarán determinadas por las siguientes premisas:</p> <ul style="list-style-type: none"> ✓ Minimizar el riesgo en los procesos de “GIVAUDAN”. ✓ Cumplir con los principios de seguridad de la información. ✓ Cumplir con los principios de la Protección de Datos Personales, consagrados en la Ley 1581 del año 2012, el Decreto único Reglamentario del Sector Comercio, Industria y Turismo, (D.U.R. 1074 del año 2015) y demás normas que las sustituyan, complementen, modifiquen o adicionen. ✓ Mantener la confianza de los clientes, proveedores y terceros. ✓ Apoyar la innovación tecnológica. ✓ Proteger los activos tecnológicos. ✓ Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información. ✓ Garantizar la continuidad del negocio frente a incidentes. 	<p>19.6.1. Scope</p> <p>For "GIVAUDAN", the protection of information aims to maintain a level of exposure, in accordance with the corporate purpose it develops, which allows it to respond for the integrity, confidentiality and availability of this.</p> <p>In accordance with the above, this policy applies to managers, employees, suppliers, customers and in general to any person who has access to the information processed by "GIVAUDAN", will be determined by the following premises:</p> <ul style="list-style-type: none"> ✓ Minimize risk in "GIVAUDAN" processes. ✓ Comply with information security principles. ✓ Comply with the principles of Personal Data Protection, enshrined in Law 1581 of 2012, the Single Regulatory Decree of the Commerce, Industry and Tourism Sector, (D.U.R. 1074 of 2015) and other rules that replace, supplement, modify or add to them. ✓ Maintain the trust of customers, suppliers and third parties. ✓ Support technological innovation. ✓ Protecting technology assets. ✓ Establish policies, procedures, and instructions on information security. ✓ Ensure business continuity in the event of incidents.

19.6.2. Políticas de seguridad de la información.

- Las responsabilidades frente a la seguridad de la información serán definidas, compartidas, publicadas y aceptadas por cada uno de los directivos y colaboradores de "GIVAUDAN".
- "GIVAUDAN" protegerá la información creada, procesada, transmitida o resguardada por sus procesos de negocio, con el fin de minimizar impactos financieros, operativos o legales debido a un uso incorrecto de la misma. Para ello es fundamental la aplicación de controles de acuerdo con la clasificación de la información de su propiedad o en custodia.
- "GIVAUDAN" protegerá su información institucional de las amenazas originadas por factores internos y externos que afecten cualquiera de sus principios.
- "GIVAUDAN" protegerá las instalaciones de procesamiento y la infraestructura tecnológica que soporta sus procesos críticos.
- "GIVAUDAN" controlará la operación de sus procesos de negocio garantizando la seguridad de los recursos tecnológicos y las redes de datos.
- "GIVAUDAN" implementará control de acceso a la información, sistemas y recursos de red.
- "GIVAUDAN" garantizará que la seguridad sea parte integral del ciclo de vida de los sistemas de información.
- "GIVAUDAN" garantizará a través de una adecuada gestión de los eventos de seguridad y las debilidades asociadas con los sistemas de información, una mejora efectiva de su modelo de seguridad.
- "GIVAUDAN" garantizará la confiabilidad y el nivel de sensibilidad de la información que provenga de terceros y de sistemas de información con los cuales se tenga interoperabilidad.

19.6.2. Information security policies.

- Responsibilities for information security will be defined, shared, published, and accepted by each of the managers and employees of "GIVAUDAN".
- GIVAUDAN shall protect the information created, processed, transmitted, or safeguarded by its business processes, in order to minimize financial, operational or legal impacts due to its incorrect use. For this purpose, it is essential to apply controls according to the classification of the information owned or in custody.
- "GIVAUDAN" will protect its institutional information from threats originated by internal and external factors that affect any of its principles.
- "GIVAUDAN" will protect the processing facilities and technology infrastructure that support your critical processes.
- "GIVAUDAN" will control the operation of its business processes ensuring the security of technological resources and data networks.
- "GIVAUDAN" will implement access control to information, systems, and network resources.
- "GIVAUDAN" shall ensure that security is an integral part of the life cycle of information systems.
- "GIVAUDAN" will ensure through proper management of security events and weaknesses associated with information systems, an effective improvement of its security model.
- "GIVAUDAN" shall guarantee the reliability and level of sensitivity of the information coming from

• “GIVAUDAN” garantizará el cumplimiento de las obligaciones legales y contractuales establecidas.

• “GIVAUDAN” actualizará esta política, teniendo en cuenta la valoración de riesgos de procesos y de seguridad de la información. En caso de incumplimiento de las Políticas de Seguridad y Privacidad de la información, “GIVAUDAN”, iniciará las investigaciones correspondientes, y aplicará los correctivos pertinentes de acuerdo con el estado de la técnica para el momento de ocurrencia de los hechos.

19.6.3. POLITICAS ESPECÍFICAS.

19.6.3.1. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN. “GIVAUDAN”, propondrá las políticas en materia de seguridad de la información y propondrá estrategias para la divulgación de la política a todos sus colaboradores, clientes y proveedores.

19.6.3.2. GESTIÓN DE ACTIVOS DE INFORMACIÓN. “GIVAUDAN”, identificará, clasificará y etiquetará los activos de información, mediante la metodología que para estos procesos se establezcan. Los directivos y colaboradores deberán evitar la divulgación, la modificación, el retiro o la destrucción no autorizados de información almacenada en los medios. Todo directivo o colaborador, que se desvincule temporal o definitivamente de la compañía, deberá realizar la devolución de activos de información que tenga asignada y en custodia, físico o digital, al supervisor o jefe inmediato. El área de IT de “GIVAUDAN”, hará mantenimiento a los portátiles entregados a los directivos y colaboradores para el desarrollo de sus funciones, y verificará el cumplimiento de estas políticas por su parte. Es de exclusiva

third parties and information systems with which it has interoperability.

• "GIVAUDAN" shall guarantee compliance with the legal and contractual obligations established.

• GIVAUDAN" will update this policy, taking into account the assessment of process and information security risks. In case of non-compliance with the Information Security and Privacy Policies, "GIVAUDAN" will initiate the corresponding investigations and will apply the pertinent corrective measures according to the state of the art at the time of the occurrence of the facts.

19.6.3. SPECIFIC POLICIES.

19.6.3.1. INFORMATION SECURITY ORGANIZATION. "GIVAUDAN" will propose policies on information security and propose strategies for the dissemination of the policy to all its employees, customers, and suppliers.

19.6.3.2. MANAGEMENT OF INFORMATION ASSETS. "GIVAUDAN" shall identify, classify, and label the information assets, through the methodology established for these processes. Managers and employees shall avoid the unauthorized disclosure, modification, removal, or destruction of information stored in the media. Any manager or employee, who leaves the company temporarily or permanently, must return the information assets assigned to him/her and in custody, physical or digital, to the supervisor or immediate boss. The IT area of “GIVAUDAN” (Hereinafter “IT Department”) will maintain the laptops given to managers and employees for the

responsabilidad de directivos y colaboradores, tomar las medidas adecuadas para el almacenamiento y resguardo de los medios removibles, evitando accesos no autorizados, daños, pérdida de información o extravío del medio. La información que reposa en los dispositivos móviles que llegará a asignar "GIVAUDAN" a los directivos y colaboradores, es responsabilidad de quien tiene en uso el dispositivo móvil. Cuando se entreguen estos dispositivos, el departamento de Tecnologías de la Información de "GIVAUDAN", deberá eliminar los datos contenidos en el dispositivo. "GIVAUDAN", tendrá fragmentada la red, en mínimo, 3 unidades

Y:\ para guardar información que pueden ver todos los usuarios de "GIVAUDAN", de manera temporal, la cual se depurará por parte del departamento de Tecnologías de la Información de "GIVAUDAN", periódicamente.

G:\ para guardar información por cada área de "GIVAUDAN".

U:\ para que el usuario logueado guarde su información. . El departamento de Tecnologías de la Información de "GIVAUDAN", será el encargado de realizar backup de la información guardada en las unidades Y, G, V y U. o las existentes, el backup de la unidad C (disco duro del equipo) será responsabilidad del usuario.

19.6.3.3. CONTROL DE ACCESO. La creación, reactivación o desactivación de usuarios de la red o sistemas de información; al igual que los roles y permisos otorgados, los realizará, el departamento de Tecnologías de la Información de "GIVAUDAN", a través de solicitud enviada por correo electrónico del jefe inmediato y/o supervisor. El departamento de Tecnologías de la Información de "GIVAUDAN", es quien gestionará el control de acceso a través de usuario y contraseña, a la red de "GIVAUDAN", correo electrónico y a los sistemas de información que administre.

development of their functions and verify compliance with these policies on their part. It is the sole responsibility of managers and employees to take appropriate measures for the storage and safeguarding of removable media, avoiding unauthorized access, damage, loss of information or loss of the media. The information contained in the mobile devices that "GIVAUDAN" may assign to managers and collaborators is the responsibility of the person who has the mobile device in use. When these devices are handed over, the IT Department of "GIVAUDAN" shall delete the data contained in the device. "GIVAUDAN" will have the network fragmented in at least 3 units.

Y:\ to store information that can be seen by all "GIVAUDAN" users, on a temporary basis, which will be debugged by the IT Department of "GIVAUDAN", periodically.

G:\ to store information for each area of "GIVAUDAN".

U:\ for the logged in user to save his information. The IT Department of "GIVAUDAN" will oversee backing up the information saved in the Y, G and U, or V units. The backup of the C unit (hard disk of the equipment) will be the user's responsibility.

19.6.3.3. ACCESS CONTROL. The creation, reactivation, or deactivation of users of the network or information systems, as well as the roles and permissions granted, will be carried out by the IT Department of "GIVAUDAN", through a request sent by e-mail from the immediate boss and/or supervisor. The IT Department of "GIVAUDAN" will manage the access control through username and password to

En caso de retiro temporal o definitivo de cualquier directivo o colaborador de "GIVAUDAN", se deberá deshabilitar o actualizar los privilegios en los sistemas a los que el usuario estaba autorizado en caso de encargos o suplencia temporal, previa solicitud por correo electrónico al departamento de Tecnologías de la Información de "GIVAUDAN".

El departamento de Tecnologías de la Información de "GIVAUDAN", monitoreará la asignación de permisos y roles otorgados a los usuarios. Las contraseñas serán de uso personal e intransferible, y deberán ser cambiadas por los directivos y colaboradores, con frecuencia.

Los directivos y colaboradores, evitarán que las contraseñas utilizadas, sean fáciles de recordar; no estén basadas en algo que otra persona pueda adivinar fácilmente u obtener usando información relacionada con la persona, (nombres, números de teléfono y fechas de nacimiento, etc.); no sean vulnerables a ataques de diccionario (es decir, no contienen palabras incluidas en los diccionarios); estén libres de caracteres completamente numéricos o alfabéticos idénticos consecutivos; si son temporales, cambiarlos la primera vez que se ingrese. Es responsabilidad del directivo o colaborador, el uso o tratamiento dado a su usuario y contraseña. El departamento de Tecnologías de la Información de "GIVAUDAN", configurará los servidores para que semestralmente el sistema solicite al usuario cambio de contraseña. No es recomendable la utilización de la opción 'recordar contraseña'. La instalación de software en los equipos de cómputo de "GIVAUDAN", será realizada a través del usuario del administrador de la red. Toda solicitud al respecto, debe gestionarse a través de El departamento de Tecnologías de la Información de "GIVAUDAN", quien aprobará su instalación.

the "GIVAUDAN" network, e-mail and the information systems it manages.

In case of temporary or definitive withdrawal of any executive or collaborator of "GIVAUDAN", the privileges in the systems to which the user was authorized in case of temporary assignments or substitution must be disabled or updated, upon request by e-mail to the IT Department of "GIVAUDAN".

The IT Department of "GIVAUDAN" will monitor the assignment of permissions and roles granted to users. Passwords will be for personal and non-transferable use and must be changed frequently by managers and collaborators.

Managers and collaborators shall ensure that the passwords used are easy to remember; are not based on something that another person can easily guess or obtain using information related to the person (names, telephone numbers and dates of birth, etc.); are not vulnerable to dictionary attacks (i.e. do not contain words included in dictionaries); are free of completely consecutive identical numeric or alphabetic characters; if they are temporary, change them the first time they are entered. It is the responsibility of the manager or collaborator, the use or treatment given to your username and password. The IT Department of "GIVAUDAN" will configure the servers so that the system will request the user to change the password every six months. The use of the 'remember password' option is not recommended. The installation of software in "GIVAUDAN's" computer equipment will be done through the network administrator's user. Any request in this regard, must be managed through the IT Department of "GIVAUDAN", who will approve its installation.

19.6.3.4. NO REPUDIO. Para ingresar a los sistemas de información que administra “GIVAUDAN”, los directivos y colaboradores deben tener su propio usuario y contraseña, se entenderá que las transacciones que se generen con este son avaladas por el servidor que tiene a su cargo dicho usuario.

19.6.3.5. PRIVACIDAD Y CONFIDENCIALIDAD. “GIVAUDAN”, se compromete a mantener reserva sobre la información que tenga acceso con ocasión del cumplimiento de obligaciones legales y contractuales. En este sentido, “GIVAUDAN”, sus directivos y colaboradores, deberán abstenerse de publicitar o utilizar información que se les entregue, como resultado del desarrollo del objeto social de “GIVAUDAN”.”

19.6.3.6. MANEJO DE EQUIPOS. “GIVAUDAN”, contará con equipos de protección (firewall) desde y hacia internet para proteger la integridad y confidencialidad de la información. Ningún usuario de “GIVAUDAN”, podrá instalar software sin licencia, solo podrá ser autorizado por el departamento de Tecnologías de la Información de “GIVAUDAN”, quienes revisarán en los mantenimientos preventivos este tema, de acuerdo con lo establecido en el Procedimiento Mantenimiento Correctivo y Preventivo. Ningún equipo podrá ser retirado de su sitio sin autorización del departamento de Tecnologías de la Información de “GIVAUDAN”. Todo computador, servidor, dispositivo de comunicaciones como switches, enrutadores o cualquier otro hardware que requiera ser conectado a la red, debe tener la autorización y supervisión del departamento de Tecnologías de la Información de “GIVAUDAN”. El departamento de Tecnologías de la Información de “GIVAUDAN”, realizará mantenimiento preventivo a los equipos de cómputo de propiedad de “GIVAUDAN”. Los directivos y colaboradores, no están autorizados para

19.6.3.4. NON-REPUDIATION. To access the information systems managed by "GIVAUDAN", managers and collaborators must have their own username and password, it shall be understood that the transactions generated with this are endorsed by the server in charge of such user.

19.6.3.5. PRIVACY AND CONFIDENTIALITY. "GIVAUDAN", undertakes to maintain the confidentiality of the information it has access to comply with legal and contractual obligations. In this sense, "GIVAUDAN", its directors, and collaborators, shall refrain from publicizing or using information given to them, because of the development of the corporate purpose of "GIVAUDAN".

19.6.3.6. EQUIPMENT MANAGEMENT. "GIVAUDAN", will have protection equipment (firewall) to and from the Internet to protect the integrity and confidentiality of the information. No user of "GIVAUDAN" may install unlicensed software, it may only be authorized by the IT Department of "GIVAUDAN", who will review this issue in preventive maintenance, in accordance with the provisions of the Corrective and Preventive Maintenance Procedure. No equipment may be removed from its place without authorization from the IT Department of "GIVAUDAN". Any computer, server, communications device such as switches, routers or any other hardware that needs to be connected to the network, must have the authorization and supervision of "GIVAUDAN"'s IT Department. The IT Department of "GIVAUDAN" will perform preventive maintenance to the computer equipment

efectuar algún tipo de intervención, reparación y/o modificación en un equipo a su cargo. El mantenimiento preventivo y correctivo debe ser realizado por El departamento de Tecnologías de la Información de "GIVAUDAN".

19.6.3.7. SEGURIDAD DE LAS OPERACIONES. El departamento de Tecnologías de la Información de "GIVAUDAN" realizará seguimiento al tráfico de la red especialmente cuando se tenga evidencia de actividad inusual o detrimentos en el desempeño. Todos los equipos de cómputo de "GIVAUDAN", deberán tener instalado software de antivirus licenciado y actualizado. El departamento de Tecnologías de la Información de "GIVAUDAN", mantendrá actualizado el procedimiento de Administración de la red y comunicaciones de "GIVAUDAN". El departamento de Tecnologías de la Información de "GIVAUDAN", establecerá los siguientes procedimientos y/o guías: Mantenimiento Preventivo, Administración de Usuarios, Copias de Seguridad y Restauración de Información, Administración de la red y comunicaciones. El departamento de Tecnologías de la Información de "GIVAUDAN" establecerá e implementará controles para evitar la descarga de software no autorizado, la infección con código malicioso proveniente de internet y el acceso a sitios catalogados como restringidos y de alta peligrosidad. Los directivos y colaboradores de "GIVAUDAN", deben evitar la descarga de software, archivos, música, juegos o videos desde internet que puedan saturar el canal dedicado de internet, disminuir la velocidad de transmisión o llegar a ocasionar algún daño en el equipo.

Los directivos y colaboradores de "GIVAUDAN", usarán los recursos y servicios de internet para asuntos institucionales. El uso personal no debe interferir con la operación eficiente de los sistemas de "GIVAUDAN", ni con los deberes y obligaciones de directivos y colaboradores. El acceso a

owned by "GIVAUDAN". Managers and collaborators are not authorized to carry out any type of intervention, repair and/or modification in the equipment they are in charge of. Preventive and corrective maintenance must be performed by "GIVAUDAN"'s IT Department.

19.6.3.7. SECURITY OF OPERATIONS. The IT Department of "GIVAUDAN" will monitor network traffic, especially when there is evidence of unusual activity or detrimentos in performance. All "GIVAUDAN" computer equipment must have licensed, and updated antivirus software installed. The IT Department of "GIVAUDAN" shall keep "GIVAUDAN"'s network and communications administration procedure up to date. The IT Department of "GIVAUDAN" will establish the following procedures and/or guidelines: Preventive Maintenance, User Administration, Backup and Restoration of Information, Network Administration and Communications. The IT Department of "GIVAUDAN" shall establish and implement controls to prevent the downloading of unauthorized software, infection with malicious code from the Internet and access to sites classified as restricted and highly dangerous. "GIVAUDAN" managers and collaborators must avoid downloading software, files, music, games, or videos from the Internet that may saturate the dedicated Internet channel, decrease the transmission speed or cause any damage to the equipment.

"GIVAUDAN" officers and employees shall use Internet resources and services for institutional matters. Personal use must not interfere with the efficient operation of "GIVAUDAN" systems, nor

internet a través del WIFI de “GIVAUDAN”, sólo será autorizado para computadores portátiles y la clave solo puede ser ingresada por personal autorizado del departamento de Tecnologías de la Información de “GIVAUDAN”.

19.6.4. COPIAS DE SEGURIDAD Y RESPALDO. Se deberán realizar y mantener copias de seguridad de la información de “GIVAUDAN”, bases de datos e información de las unidades de red, dentro y fuera de la “GIVAUDAN”. El departamento de Tecnologías de la Información de “GIVAUDAN”, establecerá un procedimiento o guía para realizar copias de seguridad, restauración y migración de la información. Todos los sistemas de información que componen la plataforma de “GIVAUDAN”, deberán incluir la documentación necesaria para garantizar la ejecución de tareas de recuperación de la información.

19.6.5. GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN. “GIVAUDAN” establecerá un mecanismo para el reporte, registro y tratamiento de los incidentes de seguridad de la información que se presenten.

19.6.6. CAPACITACIÓN Y SENSIBILIZACIÓN EN SEGURIDAD DE LA INFORMACIÓN.

Todos los directivos y colaboradores de “GIVAUDAN”, deben recibir sensibilización para tomar conciencia de la seguridad de la información y sus responsabilidades. Se debe fortalecer la cultura del manejo de contraseñas para los diferentes sistemas, aplicativos o herramientas que tiene “GIVAUDAN”.

with the duties and obligations of managers and collaborators. Internet access through "GIVAUDAN's" WIFI will only be authorized for laptops and the password can only be entered by authorized personnel of "GIVAUDAN's" IT Department.

19.6.4. SECURITY COPIES AND BACKUP. Backup copies of "GIVAUDAN's" information, databases, and information of the network units, inside and outside "GIVAUDAN" shall be made and maintained. The IT Department of "GIVAUDAN" shall establish a procedure or guide to perform backups, restoration, and migration of information. All the information systems that make up the "GIVAUDAN" platform shall include the necessary documentation to guarantee the execution of information recovery tasks.

19.6.5. INFORMATION SECURITY INCIDENT MANAGEMENT. "GIVAUDAN" shall establish a mechanism for the reporting, recording and treatment of information security incidents that occur.

19.6.6. INFORMATION SECURITY TRAINING AND AWARENESS.

All managers and employees of "GIVAUDAN" must be made aware of information security and their responsibilities. The culture of password management for the different systems, applications or tools that "GIVAUDAN" has must be strengthen