



Policies and General Information:
GBM Privacy and Personal Data Processing

1. Purpose: This document defines the practices for the custody and protection, processing, and privacy of personal data, applicable to all companies in the GBM business group:

- General Business Machines Corporation
- General Business Machines Colombia, S.A.S.
- GBM de Costa Rica, S.A.
- G.B.M. de Nicaragua, S.A.
- GBM de Panamá, S.A.
- GBM de El Salvador, S.A. de C.V.
- GBM de Honduras, S.A.
- GBM de Guatemala, S.A.
- GBM Dominicana, S.A.

2. Scope: This policy seeks to comply with the following regulations:

2.1 Regulations:

- 2.1.1. General Data Protection Regulation (GDPR): Link to complete regulation: <https://gdpr-info.eu>
- 2.1.2. Costa Rica Personal Data Protection Law – No. 8969. Link to the complete regulation: http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?param1=NRTC&nValor1=1&nValor2=70975&nValor3=85989
- 2.1.3. Regulations to the Law on the Protection of Individuals with regard to the Processing of Personal Data – Decree No. 37554-JP. Link to the complete regulation: http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?nValor1=1&nValor2=74352
- 2.1.4. Panama Law 81: Link to the complete regulation: https://s3-legispan.asamblea.gob.pa/legispan/NORMAS/2010/2019/LEY/Administrador%20Legispan_28743-A_2019_3_29_ASAMBLEA%20NACIONAL_81.pdf
- 2.1.5. Regulations to Law 81 of Panama – Executive Decree 285 of 2021. Link to the complete regulation: https://www.gacetaoficial.gob.pa/pdfTemp/29296_A/85281.pdf
- 2.1.6. Colombian Statutory Law 1581 of 2012 on Personal Data Protection. Link to the complete regulation: <https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981>
- 2.1.7. Partial regulation of Colombia's Statutory Law 1581 on Personal Data Protection – Decree 1377 of 2013. Link to the complete regulation: <https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=53646>
- 2.1.8. Law 172-13 on Personal Data Protection, Dominican Republic. Link to the full regulation: <https://www.tribunalconstitucional.gob.do/transparencia/marco-legal/leyes/ley-172-13/>

2.2 Databases

- 2.1.9. SAP CRM – Person in charge: Digital Systems Lead
- 2.1.10. SAP ERP – Person in charge: Digital Systems Lead
- 2.1.11. Smart and Simple – Person in charge: Internal Infrastructure Engineer
- 2.1.12. Jazz – Person in charge: Talent Acquisition Coordinator
- 2.1.13. Marketing database – Person in charge: Marketing and Operations Manager
- 2.1.14. Customer Journey Data Service (CJDS) Database – Person in charge: Infrastructure & Security Manager



Policies and General Information: GBM Privacy and Personal Data Processing

2.3 Responsible and in charge of the databases:

Database Controller and Processor:

GBM shall be the **controller** of the databases indicated in the “Databases” section of this policy, with responsibility for the processing of these databases. This responsibility shall include: decisions regarding the data, the purpose, the content, the means of processing, and the use of the information, based on the regulations indicated in this policy.

The **person in charge** of the Database is specified next to each Database in the “Database” section of this document.

2.4 Aplicability of Database Regulations:

Applicability of Database Regulations:

The applicability of this Policy is defined by the interrelationship between the Databases owned by GBM and their corresponding content, and the applicable regulatory guidelines of each country where GBM, its affiliates, and subsidiaries are located.

In compliance with GDPR regulations, it applies to databases formally established for the custody of personal data, which store personal data of European citizens residing in European Union countries.

In accordance with the regulations of the Republic of Costa Rica, it is indicated that it applies to personal data in databases that are used for commercial purposes, with effects in the national territory or where national law applies, or for professional purposes, respecting informational self-determination.

Panama's regulatory criteria is that it applies to databases located in the territory of the Republic of Panama that store or contain personal data of nationals or foreigners, or where the data controller is domiciled in the country.

In accordance with Colombian regulations, it applies to personal data in databases and any use thereof, provided that it is for commercial purposes with effects in the national territory or that national law applies, or for professional purposes, respecting informational self-determination.

And finally, based on the applicability set forth in the regulations of the Dominican Republic, it applies to personal data in databases and/or any use thereof, provided that they are for commercial purposes with effects in the national territory or that Dominican national law applies, respecting informational self-determination

Applicability of Regulations to GBM Personal Data Databases

	Jazz	BD Marketing	SAP CRM	SAP ERP	Smart & Simple	CJDS
GDPR	X		X			
Costa Rica Law 8969		X				
Panamá Law 81		X	X	X	X	X
Colombia Law 1581 de 2012		X		X		
Dominican Republic Law 172-13		X				



Policies and General Information:
GBM Privacy and Personal Data Processing

3. Definitions:

- Personal Data: Any information concerning natural persons that identifies them or makes them identifiable.
- Data Storage: Preservation or custody of Data in a database established in any medium provided, including Information and Communication Technologies (ICTs).
- Database: An ordered set of data of any nature, regardless of format, method of creation, organization, or storage, which allows the data to be linked together and processed or transmitted by its custodian.
- Data Processing: Any operation or set of operations or technical procedures, whether automated or not, that allows data to be collected, stored, recorded, organized, processed, selected, extracted, compared, interconnected, associated, dissociated, communicated, transferred, exchanged, transmitted, or canceled, or used in any other way.
- Personal Data Owner:
- *General Data Protection Regulation (GDPR)*: A European Union regulation that establishes rules for the protection of European citizens' personal data.
- *Personally Identifiable Information (PII)*: A set of data that makes up an individual's personal information and can lead to their unique identification.

4. General Policies:

- 4.1. This policy is covered by document ***PG-SDI-001 "Information Security Policy."***
- 4.2. GBM will obtain the signature of an Informed Consent from the data subject in a medium, preferably written, informing them of the purpose and processing of the data, indicating the existence of a Database, the processing policies, how to access it, and the purpose for the safekeeping and processing of personal data.
- 4.3. Data subjects shall have the right to:
 - Know, update, and rectify their Personal Data.
 - Request proof of the informed consent granted.
 - Be informed, upon request, regarding the use of their Personal Data.
 - File complaints for violations of the provisions of the law
 - Revoke informed consent and/or request the deletion of data.
 - Access their Personal Data that has been processed free of charge.
- 4.4. In the case of the processing of personal data of minors for the purpose of professional internships with GBM, the provision of these data subjects must be supported by an agreement between GBM and the corresponding educational institution. The personal data provided will be solely those necessary to carry out the contractual relationship for the professional internship. Personal data provided by minors is processed under the guidelines of this Policy, with the corresponding security measures, and is considered sensitive data.
- 4.5. GBM will inform the personal data subject of any security breach, including the internal Information Security Incident ticket number and the actions planned to mitigate the breach. IN-SDI-007 - Information Security Incident Management.
- 4.6. The personal data subject will be allowed to request data deletion.
- 4.7. GBM reserves the right to reject personal data deletion requests from active employees, and this is supported by the Informed Consent for Personal Data Processing signed by each employee.



Policies and General Information:
GBM Privacy and Personal Data Processing

- 4.8. GBM will only use personal data internally and will not transfer data to third parties without proper authorization. However, GBM offers the option of data portability through a CSV file if the data subject requests it.
- 4.9. In the event of an international data transfer, a personal data transfer consent form will be drawn up, specifying the scope, activities, and obligations of the data controller. This document reflects and accepts the data handling policy and guarantees appropriate action, security, and confidentiality.
- 4.10. Database managers or administrators must update the data annually and also delete any data deemed obsolete.
- 4.11. The company will adopt the technical measures it deems necessary to protect the databases.

5. Specific Requirements by Regulation:

5.1. Colombia - Statutory Law 1581 of Colombia for the Protection of Personal Data and Decree 1377 of 2013:

- 5.1.1. Applies to personal data in databases and any use thereof, provided that they are for commercial purposes with effects in the national territory or national law applies, or for professional purposes; respecting informational self-determination.
 - It does not cover personal or domestic purposes that are not commercialized. It also does not cover purposes of state criminal law, national security and intelligence, or those linked to money laundering and terrorism, journalistic or editorial information, financial and credit information, and public censuses or civil registries.
 - 5.1.2. The Data collected includes, but is not limited to, the following: first and last name, nationality, marital status, sex, age, identification number, physical and email addresses, military service card, professional identification card, signature, fingerprint, date and place of birth, contact telephone number, employment and academic history, medical information in case of emergency, references from employment, family members, and information related to other companies or public entities; recent photographs, images from surveillance cameras; essential information from the occupational examination, position, or profession of the spouse, permanent partner, parents, or any family member in case of an apparent conflict of interest.
 - 5.1.3. Considering the characteristics of the Company, the activities it carries out, and the purposes described in this Policy, the Company is required to process certain Sensitive Data in the manner and under the conditions indicated throughout this document. However, the Data Subject has the right not to answer any questions asked and not to provide such Data.
 - 5.1.4. There must be a person who processes the data on behalf of the data controller, whose duties are:
 - To update, rectify, or delete the data in a timely manner, as appropriate, and within 5 days at the request of the data processor.
 - To refrain from circulating information that is disputed by the data subject and blocked by the Superintendency of Industry and Commerce.
 - 5.1.5. There must be a person who decides on the data and its processing. Their duties are:
 - To document and record the authorization.
 - To guarantee the truthfulness, completeness, accuracy, timeliness, verifiability, and comprehensibility of the information to the data processor.
 - To update the information promptly when there are new developments or to rectify it when it is found to be incorrect, to the data processor.
 - To communicate to the data processor any information relevant to the authorized processing.
 - Inform the data processor of any questions or complaints.
- .1.1. Common duties of the data controller and the data processor:



Policies and General Information:
GBM Privacy and Personal Data Processing

- Provide access to the collected data and revoke its ownership (habeas data).
- Preservation and safeguarding of the information to prevent loss, tampering, or unauthorized or fraudulent use.
- Process inquiries and complaints.
- Inform the Superintendency of Industry and Commerce when security code violations occur and risks arise in the management of Data Subjects' information.
- Comply with the Superintendency of Industry and Commerce.

5.1.6. Restrict access to data to authorized individuals only

5.1.7. Develop an internal manual of policies and procedures for the processing of personal data.

- This manual must be registered in the National Database Registry.

5.1.8. Transfer Prohibition: Verify the data protection level of the destination country for the transfer.

5.1.9. Transmission Prohibition: Verify the data protection level of the destination country for the transfer.

5.1.10. Draw up a personal data transfer contract outlining the scope, activities, and obligations of the data controller, reflecting and accepting the data management policy, and ensuring appropriate action, security, and confidentiality.

5.1.11. Database Queries:

- Provide a procedure and means for querying information.
- Provide information on the individual record or the owner's identification.
- Maintain proof of queries.
- The owner must exhaust all complaints with the responsible party and/or the person in charge before proceeding with the Superintendency of Industry and Commerce.

5.1.12. Complaints:

- Seek correction, updating, or deletion.
- Provide a procedure and means of filing complaints regarding the information.
- Prevent incomplete complaints.
- Label the information as "complaint in process" and provide the reason.
- The owner must exhaust complaints with the responsible party and/or the person in charge before proceeding with the Superintendency of Industry and Commerce.

5.1.13. Describe the procedure used for collecting personal data, the purposes of the collection, and the relevance of the data to the case.

5.1.14. Demonstrate the use of appropriate and effective measures, considering the legal nature of the data controller, the nature of the data, the type of processing, and the potential risks of processing.

5.1.15 Register the database in an orderly manner with the Colombian National Database Registry and keep it updated.

- The data controller must provide the legal entity's data: name or business name, tax identification number, location, and contact information; or personal data if the data controller is a natural person.

5.2. European Union - GDPR:

5.2.1. Applies to formally established databases for the safekeeping of personal data, which store personal data of European citizens residing in European Union countries.



Policies and General Information:
GBM Privacy and Personal Data Processing

- 5.2.2. European Union citizens must have full visibility into the data we hold about them.
- 5.2.3. The service provider must consider data privacy by default from the design of the solution.
- 5.2.4. PII (Personally Identifiable Information) must be properly protected in a way that preserves an individual's anonymity.
- 5.2.5. The service provider must have data retention and destruction policies.
- 5.2.6. There must be a process in place to notify the authorities and the affected user within 72 hours of a personal information breach.

5.3. Panamá – Law 81 and Executive Decree 285:

- 5.3.1. Applies to databases located within the territory of the Republic of Panama, which store or contain personal data of nationals or foreigners, or where the data controller is domiciled in the country.
- 5.3.2. Applies if the processing of personal data is necessary to fulfill a contractual obligation.
- 5.3.3. Personal data retention periods must be determined.
- 5.3.4. When applicable, a record of data transfer to third parties must be maintained
- 5.3.5. There must be secure management and transfer protocols, processes, or procedures that protect the rights of data subjects.
- 5.3.6. If personal data is processed online, the privacy and service conditions must be communicated to the data subjects.
- 5.3.7. A data deletion procedure must be established once the contractual relationship with the client has ended.

5.4. Costa Rica – Law No. 8969 and Decree No. 37554-JP:

- 5.4.1. Applies to personal data in databases used for commercial purposes; with effect in the national territory or where national law applies, or for professional purposes; respecting informational self-determination.
 - Does not cover internal, personal, domestic, or non-commercial purposes.
- 5.4.2. Information must be updated or deleted promptly when there are new developments, or rectified when it is found to be incorrect, within a period of 5 business days.
- 5.4.3. Adopt technical and organizational measures to guarantee data security, including updated physical and logical mechanisms for preserving and safeguarding information to prevent loss, tampering, or unauthorized or fraudulent use.
- 5.4.4. Requests from Prodhav (Inhabitants' Data Protection Agency) must be processed, including compliance with requests to view, update, rectify, and delete data; and information that is disputed by the data subject and blocked by Prodhav must not be circulated.
 - GBM will address complaints filed with Prodhav authorities, comply with imposed precautionary measures, or respond to collection processes in the event of noncompliance with a sanction.
 - The Personal Data Processing Policy and Procedure must be registered with Prodhav.
 - The Database must be registered with Prodhav.
 - Prodhav will notify GBM via email at support@gbm.net (Service Desk).
- 5.4.5. A description of the type of personal data processed must be documented.
- 5.4.6. An inventory of the technological infrastructure containing the personal data database must be created and updated.



Policies and General Information:
GBM Privacy and Personal Data Processing

- 5.4.7. The purposes and uses of the database must be documented. Types of personal data processed and the data collection procedure; also a description of the processing technique and security measures.
- 5.4.8. The following are grounds for a complaint by a data subject to Prodhab:
- Insufficient information is provided to the data subject.
 - Insecure mechanisms or mechanisms without a guarantee of inalterability.
 - Lack of informed and express consent from the data subject.
 - Transfer of data contrary to regulations or without consent.
 - Purposes other than those declared.
 - Unjustified refusal to grant the data subject access to the data.
 - Unjustified refusal to delete or rectify data.
 - Lack of consent for sensitive data.
 - Bad faith or violence in obtaining data.
 - Lifting of confidentiality contrary to regulations.
 - Failure to register with Prodhab.

5.5. Dominican Republic – Law N172-13

- 5.5.1. Applies to personal data in databases and/or any use for which it is given, provided that it is for commercial purposes with effects in the national territory or Dominican national law applies; respecting informational self-determination.
- It does not cover personal or domestic purposes that are not commercialized. It also does not cover purposes of state criminal law, the death penalty, or merely employment-related purposes and those of the corresponding organization.
- 5.5.2. The need to obtain informed consent does not apply to: publicly accessible sources, marketing purposes, or those derived from commercial, employment, contractual, or professional relationships.
- 5.5.3. Due diligence in data processing:
- Update, rectify, or delete data promptly, as appropriate, at the data subject's request within 10 business days.
 - In the event of an assignment or transfer, notification of the rectification must be made within 5 business days.
 - In case of inquiries or complaints, label the relevant information with "complaint under review" or "disputed information."
- 5.5.4. GBM will implement procedures to comply with the following requests for action on the applicable databases:
- Process the data subject's inquiries and/or complaints.
 - Ensure the truthfulness, completeness, accuracy, timeliness, verifiability, and comprehensibility of the information.
 - Restrict access to authorized parties only.
 - Preservation and safeguarding of the information by implementing the necessary measures to prevent loss, tampering, unauthorized access, access, or use.
 - Update, rectify, or delete data promptly, as appropriate, at the data subject's request within 10 business days.
 - Act in accordance with professional secrecy, even after the relationship has ended.
 - Provide the data subject access to their data with proof of identity, within 5 business days.



Policies and General Information:
GBM Privacy and Personal Data Processing

- Provide the data subject access to their information, even if the data subject's request is deemed negative, or make ordered modifications if the data subject's claims are not pursued, if legal action is taken.
- Keep data up-to-date and correct or delete it as appropriate.
- 5.5.5. In the event of cancellation of the reason for data processing, the data will be deleted once the statute of limitations expires, except for ongoing legal obligations.
- 5.5.6. In the case of Interns or Professional Internships within GBM (always within the scope of applicable regulations), the processing of personal and sensitive data will safeguard the rights of children and adolescents.
 - GBM will ensure the protection of their physical, moral, psychological, and intellectual development, their honor, and their reputation, and that this does not constitute arbitrary or unlawful interference in their private life and family privacy or that may stigmatize their conduct or behavior.
- 5.5.7. GBM will be responsible for preventing:
 - The intentional or malicious insertion of false data.
 - The intentional or malicious provision of false information to a third party.
 - Unauthorized access to the database, violating confidentiality through malicious intent or in bad faith.
 - Disclosing confidential information when required to do so.
 - Fraudulent and unauthorized access to the database through malicious intent or in bad faith.
 - Violation of obligations through malicious intent or in bad faith.

End of Document