

1 OBJECTIVE

- 1.1 This International Personal Data Protection Policy (the “Policy”) describes Grupo Proeza, S.A.P.I. de C.V. and its subsidiaries and affiliates (“Proeza”) general privacy practices and guides for the processing of any personal data in all of Proeza’s jurisdictions.
- 1.2 This Policy aims to state the appropriate security measures applicable for the protection of personal data.

2 SCOPE

- 2.1 This Policy is applicable to all companies in Proeza including all regions and sites.

3 GUIDELINES

3.1 Personal Data Principles

- I. **Accuracy:** Personal data must be accurate and kept by the data controller.
- II. **Consent:** Personal data must be processed with prior data subject’s consent, unless other lawful bases or exceptions apply.
- III. **Data minimization/Proportionality:** Personal data must be limited to what is necessary in relation to the purpose.
- IV. **Integrity, security and confidentiality:** Personal data must be processed in a manner that provides appropriate security.
- V. **Lawfulness and fairness:** Personal data must be processed in accordance with the lawful bases for its processing.
- VI. **Purpose:** Personal data must be collected for specific, explicit and legitimate purposes.
- VII. **Quality:** Personal data must be adequate, pertinent and not excessive.
- VIII. **Storage limitation:** Personal data must be kept no longer than is necessary for the purposes.
- IX. **Transparency:** Proeza must inform the data subject, in an easily accessible form and clearly understandable.

3.2 Privacy Notices

- I. Proeza through its departments will make available to the different data subjects a privacy notice depending on the type of data subject concerned either directly or indirectly in person.

3.3 Data Subject Rights

- I. Under applicable law data subjects may be entitled to exercise one or more of the following rights, which may vary depending on the jurisdiction. These rights may be exercised by contacting Local Data Protection Officer (“DPO”).
 - a) Access; Erasure/Cancellation; Correction/Rectification; Objection/Opposition and Portability.

3.4 Data Subject Rights Procedure

- I. A request may be submitted using the email address mentioned in the privacy notice. These requests must be attended by Proeza’s local data protection officer in each jurisdiction where Proeza has operations (“Local DPO”) in order to avoid a personal data transfer.
- II. Upon receipt of the request the Local DPO should perform the procedure described below:
 - a) Identification and classification of the request.
 - b) Assess whether the data subject has right to enforce the exercised right.
 - c) Notify the data subject.
 - d) Record information and store it.
- III. The steps stated above, should be done only by Proeza’s Local DPO in the relevant jurisdiction.

3.5 Personal data transfers.

- I. Proeza endeavors to ensure that appropriate safeguards are implemented to secure such data transfers in conformity with applicable laws.

3.6 Provision of personal data to organizations that perform services on behalf of Proeza.

- I. Personal data should only be provided to organizations that perform services on behalf of Proeza with appropriate security measures that have entered into a service agreement with Proeza.

3.7 Personal data Inventories.

- I. Proeza through its departments is bound to maintain personal data inventories, and all its employees, directors, advisors, representatives, and/or outsourced employees (the “Collaborators”) must keep records accurate and up to date. The information recorded should contain information depending its jurisdiction and may be audited by Local DPO.

3.8 Record Retention

- I. Proeza is committed to collecting and processing personal data responsibly and in accordance with the storage limitation principle. Collaborators should not keep personal data for any longer than is necessary for the purpose(s) for which Proeza originally collected it.

3.9 Collaborators Personal Data

- I. Collaborators personal data may be processed in a number of ways including, but always in strict attachment to the [Global Employees Privacy Notice \(Annex 1\)](#) and this Policy.

3.10 Incidents

- I. All incidents involving the potential loss of personal data, Proeza's data or Proeza's systems in any department are considered of high priority. Incidents require the immediate engagement of the Local DPO, and the local Legal Department to assist in guiding Proeza's required actions in the jurisdictions where Proeza operates, including regulatory obligations.
- II. In case an incident involves any significant damage to data, subjects' economic or moral rights must be as soon as possible informed to Proeza's Global Data protection officer. (the "Global DPO").

3.11 Incident response process

- I. Identification: The goal of the identification phase is to gather and analyze event data, and determine if an Incident should be reported. Identification of an Incident in a timely manner is critical. In this phase, the following issues must be covered:
 - a) Incident location.
 - b) Incident source.
 - c) Data affected.
 - d) Operational impact.
 - e) Potential breach impact.
 - f) Local notification requirements.
 - g) Incident timeliness (the actual incident is concluded or ongoing)
- II. Containment: The goal of the containment phase is to get control of the situation and limit the impact or any damage that may be occurring. All containment activity must ensure that proper evidentiary is collected and chain of custody processes are followed. In this phase the following issues must be covered:
 - a) Ensure ongoing documentation of all activity.
 - b) Create forensic Images.
 - c) If external resources are engaged, provide them access.
 - d) If internal, image memory and relevant hard drives.
- III. Eradication: The goal of the eradication phase is to completely and safely remove malicious code or other incident artifacts remnant on any system. In this phase, the following issues must be covered:
 - a) Identify attacking hosts and attack vectors.

- b) Determine most effective manner to eradicate threat, including identification and mitigation of any potentially exploited vulnerabilities.
- IV. Recovery: The goal of the recovery phase is to get back to business as quickly as possible. In this phase the following issues must be covered:
- a) Determine appropriate recovery method, whether from clean backup, safely replacing specific files, or by rebuilding system from scratch.
 - b) Determine recovery tasks by priority and critical assets.
 - c) Determine if any security (or other) patches are required to be installed.
 - d) Determine whether any account credentials need to be changed.
 - e) Determine if any network security perimeter controls or configurations need to be implemented or modified.
- V. Lessons learned: The goal of the lessons learned phase is to document what happened and improve operations to prevent it from happening again.

3.12 Notification to Data Subjects

- I. Depending on the type of personal data or information involved in the Incident and the laws of each jurisdiction, Proeza may be required to notify affected parties data subjects, authorities or third parties, within a predetermined timeframe. The Local DPO, the local Legal Department and when applicable the Global DPO will determine whether notification is required and the Local DPO will be responsible for executing required notifications.
- II. In case the Global and/or Local DPO and the Legal Department determine that data subjects notifications are required to be provided the notification to be carried by the Local DPO should contain at least, to the extent possible: (i) a brief description of the breach; (ii) a description of the types of information that were involved in the breach; (iii) the steps affected individuals should take to protect themselves from potential harm; (iv) a brief description of what the Proeza is doing to investigate the breach, mitigate the harm, and prevent further breaches; as well as (v) contact information of the business unit. These requirements may vary depending the jurisdiction (see Annex 2).
- III. Contractual notifications: Proeza's internal and/or external Legal Department jointly with the Local DPO will review applicable contracts to determine whether notification is required to third party business partners and ensure that any notification meets applicable content and formatting requirements.
- IV. Informal commercial notifications: Proeza's internal and/or external legal counsel jointly with the Local DPO will collectively determine whether the nature and scope of the Incident warrants informal notification to business partners to lessen the risk of fraud or other negative consequences stemming from the Incident.

3.13 Media inquiries

- I. At no time, is anyone other than Proeza’s CEO or designee authorized to speak to the media or disclose information through any means (including social media, friends, etc.) about any potential Incident. Any such inquiries from any person not directly involved in handling the Incident shall be directed to the Proeza’s CEO.

3.14 Violations and Disciplinary Measures

- I. Any Collaborator, who violates any provision of this Policy, may be subject to the appropriate disciplinary action.

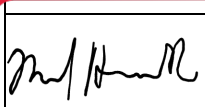


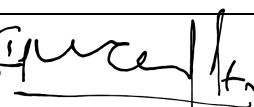
3.15 Reporting Suspected Violations

- I. Collaborators have the responsibility to report suspected violations of this Policy. Collaborators must report suspected violations through the Transparency Line and the Local DPO.

3.16 Modifications

- I. Any amendments made to this Policy must be reviewed and approved by the Ethics and Compliance Committee (“CEC”) and the Global DPO.

4 REVIEW AND APPROVAL

Version	Issue date	Elaborated by	Reviewed by	Process design validation	Authorized by
1	May 2021	Compliance Lawyer / Manuel Alejandro Herrera Rabago	Co. Legal Compliance / Fernando Perez Valdes	Co. Risk, Control and Digitalization / Gerardo Javier Sepulveda Ayala	Co. Legal and Compliance and CEC Delegate / Nicolas Villarreal Martínez
					

5 RELATED DOCUMENTS

5.1 No related documents.

6 RECORD OF CHANGES

Version	Date	Change description
1	May 2021	New document

Annex I

Global Employees Privacy Notice.

Proeza is committed to collecting and processing your personal data responsibly and in compliance with applicable data protection laws in all countries in which Proeza operates. This Global Employee Personal Data Protection Notice (“Notice”) explains how Proeza and its affiliates entities (together, “Proeza,” “we,” “us,” “our”) collect, process, transfer and disclose personal data relating to Proeza employees. This Notice also describes the rights you have regarding the use of your personal data, the measures Proeza takes to protect the security of the data, and how you can contact us regarding our data protection practices.

1. **Identifying the Controller of Your Personal Data**

Whenever a company or affiliate of Proeza collects, uses or transfers your personal data for its own purposes, that company or affiliate is considered a controller of the personal data and therefore, is primarily responsible for meeting the requirements of applicable data privacy and protection laws.

Unless informed otherwise at the time your personal data is collected, the Proeza affiliate acting as a controller of your personal data will be the one located in the country where you work, or by whom you are employed (the “Company”). The Company responsible for the collection and processing of your personal data for the purposes described in this Notice can be found in Section 10 (“Contact Us”) below.

2. **What Personal Data We Process**

During the course of your employment, the Company will collect certain personal data about you relating to your working relationship with the Company, and/or your spouse, dependents, or family members (“Dependents”), where there is a legitimate reason to do so in connection with your employment relationship, for example, to administer employee benefits. Unless the Company informs you otherwise when collecting your personal data, the provision of certain of your personal data is a requirement necessary to enter into an employment contract and/or for the performance of the employment relationship with the Company. Specific information regarding what personal data (as allowed or required under applicable law) about you the Company may process can be found below.

- PERSONAL DETAILS:** Full name (last, first, middle); official ID, birth certificate, domicile, phone number and e-mail address, tax ID, social security number; national identification number and photograph.
- COMPENSATION, STOCKS, BENEFITS AND PAYROLL DETAILS:** Annual salary; bonus information; pay frequency, amounts, dates and currency; banking details (name, address, ID/account number); payment information (credit card number, expiration date, service code).
- SENSITIVE PERSONAL DATA:** General health status, medical report results, psychometric test, criminal records, background checks, and biometric data.

To the extent permitted by applicable law, please note that you are responsible for informing Dependents whose personal data you provide to the Company about the content of this Notice.

As indicated herein, in some circumstances, it also may be necessary for the Company to process information that is regarded as special categories of personal data or sensitive data under applicable data protection law. Specifically, the Company may collect, process and use information regarding your disability (if any) or information concerning your absence due to illness, subject to the maximum extent permitted by applicable law. The Company will only process this data where it is required or authorized under applicable employment, social security or social protection laws or other applicable laws or where it is necessary to establish, exercise or defend legal claims. Where it is necessary to process such personal data for the purposes of occupational medicine or to assess your ability to work, the Company may only process such personal data by or under the responsibility of a professional subject to the obligation of professional secrecy, as required by law.

Depending on the country in which you reside, Proeza will only collect trade union membership and health-related personal data as provided by applicable data protection laws.

3. Why We Process Your Personal Data

The Company will process your personal data where the processing is necessary in connection with the performance of your employment relationship with the Company.

The Company will process your personal data for legitimate business reasons to ensure the continuity of the business.

The Company also will process your personal data for compliance with legal obligations to which the Company is subject.

The Company will not use personal data for any other purpose incompatible with the purposes described in this Notice, unless it is required or authorized by law, with your Consent, or is in your own vital interest (e.g., in the case of a medical emergency).

The Company does not sell your personal data for commercial purposes.

4. Recipients of Personal Data

Proeza will only grant access to personal data on a need-to-know basis, and such access will be limited to the personal data that is necessary to perform the business function for which such access is granted. No authorization will be extended to access personal data on a personal basis.

Access to personal data within Proeza may include your managers and their designees, personnel in HR, IT, Benefits, Proeza's Transparency Line, travel services, audit, finance, legal and compliance, or data processing departments.

From time to time, Proeza may need to make personal data available to other unaffiliated third parties. Such unaffiliated third parties may include the following:

- Professional Advisors:** Accountants, auditors, lawyers, bankers, insurers, and other outside professional advisors in all of the countries in which Proeza operates.



- **Service Providers:** Companies that provide products and services to Proeza such as IT systems suppliers and support, insurance, payroll, employee expense processing, employee benefits and rewards, credit card companies, and other service providers.
- **Public and Governmental Authorities:** Entities that regulate or have jurisdiction over Proeza such as regulatory authorities, law enforcement, public bodies, and judicial bodies, including any regulatory entities outside the country in which you work.
- **Corporate Transaction:** A third party in connection with any proposed or actual reorganization, merger, sale, joint venture, assignment, transfer or other disposition of all or any portion of Proeza's business, assets or stock (including in connection with any bankruptcy or similar proceedings).
- **Public and Private Collaborations:** Entities that seek to collaborate with Proeza either of private or public nature which are compatible with its business purpose.

5. International Data Transfers

Due to the global nature of Proeza's operations, the Company may disclose and transfer certain personal data to personnel and other departments throughout.

Unless prohibited by applicable law, personal data will be transferred to Proeza companies and affiliates in locations outside the country in which you work, where the data protection regime may be different than in the country in which you are located. Where required by applicable law, the transfer will be based on a legally adequate transfer method.

The transfers of data to third-party vendors are secured by implementing the safeguards required under the applicable data protection law (including contractual arrangements entered into with a third party vendor). Third-party service providers are expected to protect the confidentiality and security of personal data, and only use personal data for the provision of services to Proeza, and in compliance with applicable law.

6. Security Measures

Proeza maintains appropriate physical, organizational and technical security measures intended to prevent loss, misuse, unauthorized access, disclosure, or modification of your personal data under Proeza's control. If you have reason to believe that your personal data is no longer secure, please notify the Company immediately using the contact information supplied in Section 10 ("Contact Us").

7. Retention Period

Proeza retains your personal data not longer than allowed under applicable data protection laws and, in any case, no longer, than such personal data is necessary for the purpose for which it was collected or otherwise processed, unless a longer retention period is required by applicable law.

8. Your Data Protection Rights



To the extent required by applicable law, you are entitled to access and obtain information on the processing of your personal data, to object or oppose to processing of your personal data, and to have your personal data rectified or deleted/cancelled or their processing restricted. You also are entitled to withdraw any Consent that you might have given with respect to the processing of your personal data at any time with future effect "Data Subject Rights".

If you would like to exercise your data subjects rights or learn more about the processing of your personal data, please contact, us using the information provided below under Section 10 ("Contact Us"). The Company will respond to your request(s) as soon as reasonably practicable, but in any case within the legally required period of time.

If you are not satisfied with the Company's response or believe that your personal data is not being processed in accordance with the law, you also may contact or lodge a complaint with the competent supervisory authority or seek other remedies under applicable law.

9. Updating Your Personal Data

Proeza strives to maintain your personal data in a manner that is accurate, complete and up-to-date. However, as an employee, you have an obligation to keep your personal data up-to-date and inform the Company of any significant changes to your personal data.

10. Contact Us

If you have any questions or concerns regarding this Notice or to exercise your Data Subjects Rights as outlined in Section 8 above, please contact your Local Data Protection Officer.

11. Modifications

Our Notice may change when necessary. We will post any Notice changes on our site. We will also keep prior versions of this Notice in an archive for your review.

12. Consent

I hereby acknowledge receipt of this Notice and grant my express Consent for the processing of my personal data including my personal financial and economic information in terms of this privacy notice.

Name: _____

Signature: _____

Date: _____

Effective Date	Version No.	Previous Revision
____, 2021		

Annex 2 – Incident Notification

By means of this Breach Notice (the “Notification”) [***] (the “Data Controller”) hereby informs you that despite the administrative, physical and technical security measures implemented by the Data Controller, a security incident (the “Incident”) has occurred consisting in [***], its deletion and damage. As a consequence of the Incident, the following personal data was compromised: [***] (jointly, the “Personal Data”).

In this regard, we hereby recommend to implement the following measures as soon as possible, in order to protect your Personal Data, as well as your interests: ¹

1. [Contact the Data Controller in order to give notice of any improper use that has been detected on your Personal Data, and thus, avoid its improper use.]
2. [Consider making the changes that you deem appropriate regarding the handling of your Personal Data.]
3. [Remain vigilant and take steps to protect against identity theft or fraud, including monitoring your accounts and reports for signs of suspicious activity.]

Furthermore, we inform you that the Data Controller has implemented the following corrective actions, in order to protect your Personal Data:²

1. [Restored the security systems.]
2. [Modified passwords and permits to the IT personnel.]
3. [Internet access permissions on the servers exposed in the Incident have been modified. Likewise, access permissions to the opening switch were modified, to prevent unauthorized access or unauthorized use.]
4. [Firewall rules have been modified to restrict direct internal and external connections to networks.]
5. [A comprehensive review of the architecture and the need to separate document storage from the main server, as well as the implementation of documentation encryption measures, is in progress.]
6. [Carried out cybersecurity and information security breach tests to detect ongoing possible breaches in our systems.]

For further information regarding the Incident, you may personally contact the Data Controller at the following address: [***], or you may send an e-mail at the following address: [***].

We are fully committed to protecting the information that you have entrusted to us and are extremely disappointed that this Incident occurred. We will diligently work to maintain the security of your information.

¹ Examples

² Examples

Manuel Alejandro Herrera Rabago (Manuel.Herrera@proeza.com.mx) creó el documento - con dirección IP 189.208.128.231	Aug 03, 2021, 16:07:26 CST
Manuel Alejandro Herrera Rabago (Manuel.Herrera@proeza.com.mx) firmó el documento - con dirección IP 189.208.128.231	Aug 03, 2021, 16:07:26 CST
Solicitud de firma enviada a Fernando Pérez (fernando.perez@proeza.com.mx)	Aug 03, 2021, 16:08:49 CST
Solicitud de firma enviada a Gerardo Sepúlveda (gerardo.sepulveda@proeza.com.mx)	Aug 03, 2021, 16:08:49 CST
Solicitud de firma enviada a Nicolás Villarreal (nicolas.villarreal@proeza.com.mx)	Aug 03, 2021, 16:08:49 CST
Fernando Pérez (fernando.perez@proeza.com.mx) firmó el documento - con dirección IP 187.216.76.18	Aug 04, 2021, 07:44:54 CST
Gerardo Sepúlveda (gerardo.sepulveda@proeza.com.mx) firmó el documento - con dirección IP 187.162.45.153	Aug 04, 2021, 16:55:39 CST
Nicolás Villarreal (nicolas.villarreal@proeza.com.mx) firmó el documento - con dirección IP 189.159.207.219	Aug 05, 2021, 14:45:13 CST
Documento certificado por Advantage Security, S de RL de CV como Prestador de Servicios de Certificación autorizado por la Secretaría de Economía en cumplimiento a la NOM 151	Aug 05, 2021, 14:45:14 CST
Documento encriptado e integrado a Blockchain privada para integridad de documento garantizada en: https://www.weesign.mx/validation	Aug 05, 2021, 14:45:14 CST
