Security Incident Management Procedure (GDPR)

Gonvarri Industries

PROC-CORP-05

Content:

1. Objetive

The purpose of this document is to establish and communicate to all areas of Gonvarri Industries (hereinafter, GI) the procedure for notifying and managing in a standard manner the incidents that may compromise the security of the Personal Data held by GI, in compliance with the General Data Protection Regulations (GDPR).

In this regard, Regulation (EU) 2016/679 of the European Parliament and of the Council of the European Union, adopted on 27 April 2016, on the protection of individuals with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), provides that security incidents involving Personal Data must be documented and reported.

2. Scope

This procedure applies to all the companies that make up the Gonvarri Industries Group, in which the parent company, Gonvarri Corporación Financiera, S.L.U., and all the personnel of the Gonvarri Industries Group hold a majority interest, directly or indirectly, in the exercise of their functions and responsibilities, and in all the professional areas in which they represent the Group, meaning the directors, executives, employees and collaborators of the GI Group, regardless of their position, responsibility or geographical location

In any case, the Group's actions comply with the legislation in force in each jurisdiction, and therefore, in some of these jurisdictions, the principles set forth in this policy may be replaced by more restrictive laws and regulations in force.

3. Terms and Definitions

- **Processing Area:** The unit responsible for processing the data associated with the corresponding processing
- **Privacy Committee**: Unidad máxima de reporte en materia de Privacidad.
- **Personal Data:** Any information concerning identified or identifiable individuals.
- **Privacy Manager:** A natural or legal person, public authority, service or other body that, alone or with others, determines the purposes and means of processing

- **Incident:** Any anomaly involving the destruction, loss or accidental or unlawful alteration of personal data transmitted, stored or otherwise processed, or unauthorized communication or access to such data**.**

- **Privacy Officer:** Is the main person in charge of controlling and supervising compliance with privacy and data protection regulations in the organization.

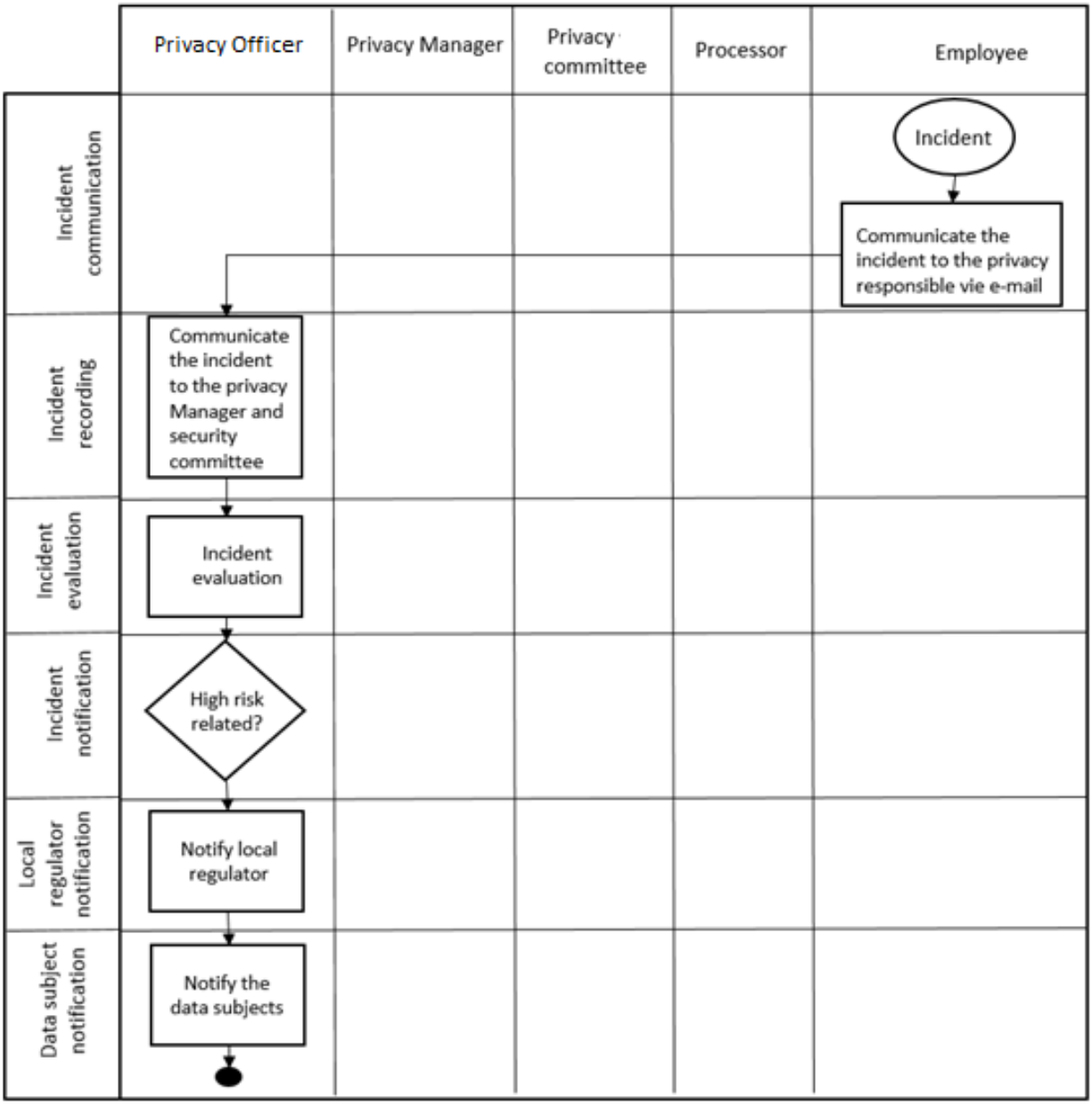
- **Data subject:** The person to whom the data belongs who is affected by the incident.

- **Data processing:** Operations and technical procedures of an automated or non-automated nature that allow for the collection, recording, storage, processing, modification, blocking and cancellation, as well as the transfer of data resulting from communications, queries, interconnections and transfers

4. Security Incident Management Procedure on Personal Data

This procedure will be carried out in the event of any incident affecting the security of Personal Data. In any case, the actions described in sections “4.1 Incident Communication”, “4.2 Incident Recording” and “4.3 Incident Evaluation” will be carried out and the actions described in section “4.4. Notification of the Incident" in cases where the security incident poses a high risk to the rights and freedoms of those affected.

The following graphically shows the general flow followed in the procedure for managing security incidents regarding Personal Data:



4.1 Incident Communication

- All staff are obliged to report any security incidents relating to personal data to the Privacy Officer. This notification will be made through the email address Privacy.Incidents@Gonvarri.com or through the form placed at the corportive website.

- Incidents may occur in all activities related to the handling and management of information in physical format or logical databases that store personal data, as well as in the development of activities that affect the security of the data contained therein

- The following are some examples of incidents:

    - Collect personal data without the consent of the data subject and without informing him/her of his/her rights.
    - Attempted or violated physical access control and databases.
    - Alter databases (deletion, modification or inclusion of data that may affect the quality of the database).
    - Removing data from media without proper authorization.
    - Extract data on media other than those authorized in the database record.
    - Failure to comply with the provisions of the Security Document for data recovery.
    - Failure to comply with the deadlines established to resolve and respond to requests to exercise the rights of the interested party.
    - Illegally using personal data.
    - Execute the data recovery process.
    - Improperly manage backups.
    - Loss of tangible assets (work phone, laptops, etc.).
    - Inability to access the system with our usual username/password.
    - Possibly compromised access password.
    - Abnormal system behaviour (incomplete or unrealistic information, unexpected failures, etc.).

- Incidents relating to personal data are not limited to automate processing, but also include means of non-automated processing. Therefore, incidents affecting such media, such as the loss of paper lists containing personal data, must also be reported and recorded by the system described in this section.

4.2 Incident Registration

Once the security incident has been reported, the following actions will be taken:

- The Privacy Officer will formally record the security incident. In this regard, at least the following information shall be detailed:

    - Type of Incident.
    - Description of the Incident.
    - Date and time of the notification.
    - User reporting the incident.

- If necessary, the Privacy Officer will coordinate with the Privacy Officer to analyse the security incident. In addition, the Privacy Officer may request technical support from department heads during the analysis phase of the incident.

4.3 Incident Evaluation

Once the security incident has been recorded, the following actions will be performed:

- The Privacy Officer will evaluate the security incident.

- In the event that the Privacy Officer deems it appropriate, based on the criticality of the incident, he or she may call a meeting of the Privacy Committee in order to evaluate the impact of the incident on the group.

- The category or level of criticality of the incident with respect to the security of the affected information. Following the generic classification, we can distinguish between:

    - Critical (affects valuable data, large volume and in a short time)
    - Very High (When you have the capacity to affect valuable information, in appreciable quantity)
    - High (When you have the capacity to affect valuable information)
    - Medium (When you have the capacity to affect an appreciable volume of information)
    - Low (Little or no capacity to affect an appreciable volume of information).

In addition, there may be technical scenarios that may lead to an incident:

- 0-day (unknow vulnerability): Vulnerability that allows an attacker to access data to the extent that it is an unknown vulnerability. This vulnerability will be available until the manufacturer or developer resolves it.

- APT (targeted attack): This refers to different types of attacks that are normally aimed at gathering fundamental information that will allow the continuation of more sophisticated attacks. This category includes, for example, an email campaign with malicious software to employees of a company until one of them installs it on their computer and provides a gateway to the system.

- Denial of Service (DoS/DDoS): It consists of flooding a system with traffic until it is not able to provide service to its legitimate users.

- Access to Privileged Accounts: The attacker gets access to the system through a user account with advanced privileges, which gives him freedom of action. Previously, the user name and password must have been obtained by some other method, such as a targeted attack.

- Malicious Code: Pieces of software whose purpose is to infiltrate or damage a computer, server, or other network device for a variety of purposes. One of the possibilities for malicious code to reach an organization is for a user to unintentionally install it.

- Compromise of Information: Collects all incidents related to access and leakage, modification or deletion of non-public information.

- Data theft and/or filtration: Included in this category is the loss/theft of storage devices with information.

- Defacement: It is a type of directed attack that consists of the modification of the corporate website with the intention of posting messages of any kind or any other intention. The normal operation of the website is interrupted, causing reputational damage.

- Exploitation of application vulnerabilities: When a potential attacker successfully exploits an existing vulnerability in a system or product by compromising an organization's application.

- Social Engineering: These are deception-based techniques, usually carried out through social networks, which are used to direct a person's behavior or obtain sensitive information. For example, the user is induced to click on a link by thinking it is the right thing to do.

If any of these events happens to occur, the security incident must be reported:

- Any local data protection regulator.
- The affected parties

4.4 Incident Notification

4.4.1. Notification to the Supervisory Authority

As mentioned above, as soon as the data controller becomes aware that a breach in the security of personal data has occurred, he must, without delay and no later than 72 hours after becoming aware of it, make the corresponding notification to the Supervisory Authority. A security breach is considered to be recorded when there is a certainty that it has occurred and there is sufficient knowledge of its nature and scope.

The criterion to be taken into account in determining whether an incident has produced "a breach in the security of personal data" is included in the GDPR itself, and includes "all those security breaches that cause the accidental or unlawful destruction, loss or alteration of personal data transmitted, stored or otherwise processed, or the unauthorized communication of or access to such data.

This communication shall be made using the communication model described in Annex , and shall contain the following information:

Identifying and contact data of:

- Entity / Person responsible for processing

- Data Protection Officer (if designated) or contact person
- Indication of whether the notification is complete or partial. In the case of a partial notification, indicate whether it is a first notification or a supplementary notification.

Information about the personal data security breach:

- Date and time of detection.
- Date and time of the incident and its duration
- Circumstances in which the personal data security breach has occurred (e.g. loss, theft, copying, etc.)
- Nature and content of the personal data.
- Summary of the incident that caused the personal data security breach (with indication of physical location and storage medium).
- Possible consequences and negative effects on those data subjects affected.
- Technical and organizational measures taken by the controller according to paragraph 33.2(d) of the GDPR.
- Category of data affected and number of records affected.
- Category and number of individuals affected.
- Possible issues of a cross-border nature, indicating the possible need to notify other supervisory authorities.
- If, at the time of notification, it is not possible to provide all the information, it may be provided at a later stage, gradually in different stages. The first notification shall be made within 72 hours, and at least one final or closing communication shall be made when all the information relating to the incident is available.
- When the data controller makes the first notification, he or she shall state whether he or she will provide further information a posteriori. He may also provide additional information by means of intermediate communications to the supervisory authority at its request, or when the data controller considers it appropriate to update the situation of the supervisory authority.
- Where initial notification is not possible within 72 hours, the notification shall also be made a posteriori and shall state and justify the reasons for the delay.
- Notifications must be clear, concise and include the information necessary for them to be properly analysed.

4.4.2. Identification of the Supervisory Authority

Where an incident may affect the data of persons in more than one Member State, the controller should make an assessment of which is the main authority to which the notification should be made and, in case of doubt, at least notify the local supervisory authority where the breach has taken place. It will act as the main supervisory authority, the main establishment or the sole establishment of the person responsible.

The criteria for identifying the main establishment are:

- The place where the main headquarter of the data responsible is located.
- The place where decisions about ends and means are made.

At the following link published by WP29, there is the contact information for each supervisory authority:

20180419_NationalDataProtectionAuthoritie

4.4.3. Notification to the Data Subjects Concerned

As in the previous section, in the event of a security incident that poses a high risk to the rights and freedoms of those data subjects concerned, this should be communicated to the affected parties in order to enable them to take measures to protect themselves from the consequences of the incident.

The Privacy Officer is responsible for notifying the affected parties of the incident and must inform them of it within a reasonable period of time.

The notification will be made by email and will include the following information:

1. Contact details of the Data Protection Officer, or where appropriate, the contact point where further information can be obtained.
2. General description of the incident and when it occurred.
3. The possible consequences of the personal data security breach.
4. Description of personal data and information affected.
5. Summary of measures implemented so far to control possible damage.
6. Other useful information to those affected to protect their data or prevent possible damage.

4.5 Exception to notification/communication

Notification to the Supervisory Authority will not be necessary where the data controller can demonstrate, in a reliable manner, that the breach in the security of personal data does not pose a risk to the rights and freedoms of natural persons.

For example, if the data were already publicly available and their disclosure does not entail any risk to the data subject.

Furthermore, communication to data subjects will not be necessary where:

- The responsible has taken appropriate technical and organizational measures, such as data not being intelligible to unauthorized persons or machines prior to the personal data security breach (through the use of: state-of-the-art data encryption, minimization, data dissociation, access to test environments without real data, etc.)

- For example, notification may not be necessary if a mobile device is lost and the personal data it contains is encrypted. However, notification may be required if this is the only copy of the personal data, or for example, the encryption key in the possession of the data controller is compromised.

- The data controller has taken protection measures that fully or partially mitigate the possible impact on those affected and ensure that there is no longer any possibility of the high risk materialising. For example, by immediately identifying and implementing measures against the person who has accessed personal data before they could do anything with it.

- When notification to those affected involves a disproportionate effort at the technical and organizational level. For example, where contact details have been lost as a result of the breach, or where a new notification system or process needs to be developed, or where excessive internal resources are required to identify data subjects concerned. In this situation, notification will be made publicly through the channels established by the data controller.

5. Responsabilities

The following is an allocation of responsibilities matrix (RACI) within the process of managing security incidents involving personal data. In this matrix, one or more responsibilities represented by a letter are assigned to each of the tasks:

- R (Responsible): This role corresponds to the person who actually performs the task.

- A (Accountable): This role is responsible for the task being performed and is accountable for its execution.
- C (Consulted): This role has some information or capacity needed to perform the task.

- I (Informed): This role should be informed about the progress and results of the task execution.

Task/Resources	Privacy Committee	Privacy Officer	Privacy manager	Area Responsible for processing	Employee
Communicate the incident	**I**	**I**	**I**	**I**	**R / A**
Record the incident	**I**	**R / A**	**I / C**	**I**	
Evaluate the incident	**I/C**	**R / A**	**I / C**	**I/C**	

Notifying local regulator	**I**	**R / A**	**I**	**I**	
Notifying the affected parties	**A**	**R**	**I**	**I**	

6. Language

This Standard is published in Spanish and English, the former being prevalent in case of divergence between the two.

7. Control of versions

Version	Date	Description	Prepared by	Review by
Version 1	30th October 2018	Initial Version of the Document	Daniel Lluch	Compliance Committee

8. Approval and entry into force

This Standard has been approved by the Compliance Committee of Gonvarri Industries Group on October the 30th of 2018, and takes effect 20 calendar days after its approval. As of the entry into force, the previous provisions existing in their case that regulate the same content are repealed.

SIGNED BY COMPLIANCE COMMITTEE

ANNEX

Security Breach Notification Form (AEPD)

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

FORMULARIO NOTIFICACIÓN BRECHAS DE SEGURIDAD

1. Datos de la notificación

Tipo de notificación: ○ Inicial, ○ Adicional, ○ Completa
Referencia notificación inicial:_____ Fecha notificación inicial:_____

2. Identificación del Delegado de Protección de Datos o persona de contacto

NIF/NIE: _____ Nombre:_____
Apellidos:_____ Cargo:_____
Dirección:_____ C.P.:_____
Provincia:_____ Localidad:_____
Teléfono(s):_____/_____ e-mail:_____

3. Identificación del responsable del tratamiento

Nombre de la Organización: _____
Tipo de Organización: ○ Privada, ○ Pública
CIF:_____ Dirección distinta del DPD o persona de contacto: ☐
Dirección:_____ C.P.:_____
Provincia:_____ Localidad:_____
Teléfono(s):_____/_____ e-mail:_____

4. Identifiación del encargado del tratamiento

¿Hay otra organización implicada en la brecha de seguridad? ☐
Nombre de la Organización: _____
Tipo de Organización: ○ Privada, ○ Pública
CIF:_____
Dirección:_____ C.P.:_____
Provincia:_____ Localidad:_____
Teléfono(s):_____/_____ e-mail:_____

5. Información temporal de la brecha

Fecha detección de la brecha: _____ ○ Exacta, ○ Estimada.
Medios de detección de la brecha:

_____
_____
_____

Justificación de notificación tardía (notificación pasadas 72h desde la detección):

_____
_____
_____

Fecha inicio de la brecha: _____ ○ Exacta, ○ Estimada.
¿Está resuelta la brecha? ☐ Fecha de resolución: _____ ○ Exacta, ○ Estimada.

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

FORMULARIO NOTIFICACIÓN
BRECHAS DE SEGURIDAD

6. Sobre la brecha

Resumen del incidente:

_____
_____
_____

Tipología:

- ☐ Brecha de confidencialidad (acceso no autorizado)
- ☐ Brecha de integridad (modificación no autorizada)
- ☐ Brecha de disponibilidad (desaparición o pérdida)

Medio por el que se ha materializado la brecha:

☐ Datos personales residuales en dispositivos obsoletos.	☐ Documentación perdida, robada o depositada en localización insegura.	☐ Eliminación incorrecta de datos personales en formato papel.
☐ Hacking.	☐ Malware (e.j. ransomware).	☐ Phishing.
☐ Correo perdido o abierto.	☐ Dispositivo perdido o robado.	☐ Publicación no intencionada.
☐ Datos personales mostrados al individuo incorrecto.	☐ Datos personales enviados por error.	☐ Revelación verbal no autorizada de datos personales.

☐ Otros:_____

Contexto:

○ Interna (acción no intencionada)	○ Interna (acción intencionada)
○ Externa(acción no intencionada)	○ Externa (acción intencionada)
○ Otros:	

Medidas preventivas aplicadas antes de la brecha:

_____
_____
_____
_____

7. Sobre los datos afectados

Categoría de datos afectados:

☐ Datos básicos	☐ Credenciales de acceso o identificación	☐ Datos de contacto
☐ DNI, NIE y/o Pasaporte	☐ Datos económicos o financieros	☐ Datos de localización
☐ Sobre condenas e infracciones penales	☐ Otros: _____	

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

FORMULARIO NOTIFICACIÓN BRECHAS DE SEGURIDAD

Categorías especiales de datos:

☐ Sobre el orígen racial ☐ Sobre la opinión política
☐ Sobre la religión o creencia ☐ Sobre la afiliación sindical ☐ Sobre la vida sexual
☐ De salud ☐ Genéticos ☐ Biométricos
☐ Desconocidos ☐ Otros: _____

Número aproximado de registros de datos personales afectados:

8. Sobre los sujetos afectados

Perfil de los sujetos afectados:

☐ Clientes ☐ Usuarios ☐ Empleados ☐ Suscriptores
☐ Estudiantes ☐ Pacientes ☐ Otros: _____

Número aproximado de personas afectadas:

9. Posibles consecuencias

Brecha de confidencialidad:

☐ Divulgación a terceros /difusión en internet ☐ Los datos pueden ser explotados con otros fines
☐ Enriquecimiento de otras bases de datos ☐ Otras: _____

Brecha de integridad:

☐ Datos han sido modificados aunque hayan quedado inservibles o irrecuperables ☐ Datos han sido modificados y utilizados para otros fines
☐ Otras: _____

Brecha de disponibilidad:

☐ Imposibilidad de la prestación de un servicio a los interesados ☐ Deterioro de las condiciones de prestación de un servicio a los interesados
☐ Otras: _____

Naturaleza del impacto potencial sobre los sujetos:

☐ Pérdida de control sobre sus datos personales ☐ Limitación de sus derechos ☐ Discriminación
☐ Usurpación de identidad ☐ Fraude ☐ Pérdidas financieras
☐ Reidentificación no autorizada ☐ Perdida de confidencialidad de datos afectados por secreto profesional
☐ Daños a la reputación ☐ Otras: _____

Severidad de las consecuencias para los individuos: ○ Baja ○ Media ○ Alta ○ Muy alta

Medidas tomadas para solucionar la brecha y minimizar el impacto sobre los afectados:

_____
_____
_____
_____
_____

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

FORMULARIO NOTIFICACIÓN BRECHAS DE SEGURIDAD

10. Comunicación a los interesados

¿Se ha comunicado la brecha a los interesados?

○Si — Fecha en la que se informó: _____

Número de sujetos informados: _____

Medios o herramientas de comunicación: _____

○No, pero serán informados — Fecha en la que se informará: _____

○No serán informados — Justificación para no informar: _____

○Pendiente de decidir

(Adjuntar contenido de la comunicación a los interesados)

11. Implicaciones trasfronterizas

¿Hay sujetos de otros Estados miembros de la UE afectados por la brecha? ☐

Marque los Estados que puedan estar afectados (A) y aquellos a los que haya notificado(N) la misma brecha de seguridad:

A	N		A	N		A	N	
☐	☐	Alemania	☐	☐	Austria	☐	☐	Bélgica
☐	☐	Bulgaria	☐	☐	Chipre	☐	☐	Croacia
☐	☐	Dinamarca	☐	☐	España	☐	☐	Eslovaquia
☐	☐	Eslovenia	☐	☐	Estonia	☐	☐	Finlandia
☐	☐	Gran Bretaña	☐	☐	Grecia	☐	☐	Hungría
☐	☐	Irlanda	☐	☐	Italia	☐	☐	Letonia
☐	☐	Lituania	☐	☐	Luxemburgo	☐	☐	Malta
☐	☐	Países Bajos	☐	☐	Polonia	☐	☐	Portugal
☐	☐	Rep. Checa	☐	☐	Rumania	☐	☐	Suecia

12. Documentos adjuntos

(Adjuntar documentos)

En_____,a___de_____20__


Gonvarri
Industries