



GPA Global Privacy and Data Protection Awards 2023

Entry Form

To submit an entry to the GPA Global Privacy and Data Protection Awards please complete and email this form to secretariat@globalprivacyassembly.org **no later than 9 June 2023**.

Note: GPA member authorities can submit as many entries as they wish, but a separate form should be used for each different entry, submitted by the deadline above.

Languages: The GPA documentation Rule 6.2¹ applies.

1. CONTACT DETAILS FOR THIS ENTRY

Privacy/Data Protection

Authority:

Agencia Española de Protección de Datos (AEPD)

Person completing this form:

Luis Antonio

de Salvador Carrasco

First name

Last name

Job title:

Director of Innovation and Technology Division

Email address:

dit@aepd.es

2. ELIGIBILITY

By submitting this entry, I confirm that (*please tick all boxes to confirm*):

- ☒ The Authority is a member of the Global Privacy Assembly
- ☒ The initiative described in this entry was undertaken since January 2022.
- ☒ I am aware that the information in the entry (other than the contact details in 1(a) above) will be publicised by the GPA Secretariat.

3. CATEGORIES

Please indicate which category you wish to enter.

*Please tick **one**; please use a separate form for each category you wish to enter:*

- ☐ Education and Public Awareness
- ☒ Accountability
- ☐ Dispute Resolution and Enforcement
- ☐ Innovation
- ☐ People's Choice

¹ [GPA Rules and Procedures](#), Rule 6.2 'Assembly documents':

Without prejudice to section 4.2, Assembly documents, including accreditation and observer applications may be submitted in English or in another language. In the latter case, the documents shall be accompanied by an English version. Members with the ability and the resources to do so are encouraged to translate proposed resolutions and other Assembly documents such as the Assembly Rules and Procedures.

4. DESCRIPTION OF THE INITIATIVE

a. Please provide a brief summary of the initiative (no more than 75 words)

GESTIONA EIPD v2 (manage DPIA) is a free web tool that assists controllers/processors to keep a record of processing activities, carries out the risk analysis of each processing, assesses the obligation/need to carry out a DPIA, and the whole risk management: it provides a set of measures and safeguards (organizational, legal, and technical) that could be taken to address each specific risk factor. It runs locally in the browser, stores locally, and generate several reports.

b. Please provide a full description of the initiative (no more than 350 words)

The purpose of this tool is to support controllers and processors, mainly SME, with a free tool that implements the management, including risk management, of their processing activities. It allows to make an assessment about the duty to carry out the DPIA. In addition, it enables a record of processing activities as required by GDPR Article 30.1.

The tool executes in a web browser, locally, without server communication, data can confidentially be saved/loaded to local files and reach up to 500 different processing. It consists of two components: the management of the data processing, and the risk management specific to each data processing:

Data processing Management: Allows to add a data processing filling in an input form. Displays the managed data processing and dumps the results of the risk assessment carried out. Several reports can be generated: record of processing activities report (GDPR Art. 30.1), and an extended report including a detailed summary of their risk assessments. (see below: *Main screen: Data processing Management*)

Data Processing Risk Assessment: After adding a new data processing, or when selecting and editing an existing one, the tool will display the screen for risk assessment, separated in different categories:

- The applicability of the different risk factors to the processing of personal data can be selected (examples are shown in some cases). Some risk factors require to indicate their likelihood and impact.
- The "Risk Management" tab displays the level of calculated intrinsic and residual risk, the assessment of the obligation to perform the EIPD, and a summary report. The management procedure to reduce the risk, by means of mitigation and control measures is also provided.
- Control and mitigation measures can be selected to address the specific identified risks. The measures proposed by the tool are classified into the following dimensions:
 - Processing concept, design and data protection by design.

- Security, failures, errors, and data breach management.
- Governance measures and data protection policies.
- Additional control measures can be entered by the user

c. Please explain why you think the initiative deserves to be recognised by an award
(no more than 200 words)

This tool allows to implement a full GDPR management of multiple processing activities without economic expenditure, is specifically adapted to SME's, in a web-based interface, with total confidentiality and portability.

It implements in a practical and easy way to understand the guidelines, checklist, templates, and lists released by the Spanish DPA (see below).

It implements the identification, assessment, and mitigation of the risks for the rights and freedoms in the processing of personal data that are defined in 35.3 GDPR, lists regarding 35.4, in the guidelines of the EDPB and other regulations.

It allows to assess the duty or the recommendation to carry out DPIAs.


The user can select from a different set of safeguards that allow to manage every specific risk factor, and to assess the residual risk.

It also generates documentation that is not only a support to comply with the GDPR but also a useful resource for any company or professional (when dealing with low-risk processing activities such as informative and contractual clauses, etc).

- d. Please include a photograph or image, if you wish (This will be published with your entry on the GPA website. The image can be pasted into the box below, be sent as an attachment or a link may be provided)

Below different screen captured that show different application stages:

Main screen (showing two data processing)



Manage DPIA v2

Data processing Records and Risk Assessment

Castellano | English ?

Save Upload Reports / Export

Data Processing Controller

A Test Company (DELETE) 12345678-TIN
Main Street, 12 28080 Madrid (SPAIN)
989 321 321 info@test-company.es
Consumer electronic services
data subject rights: dataprotectionofficer@test-company.es
(In order to change these data and DPO edit and modify the first data processing in the list)

Personal Data Processing

Personal data processing are listed below:

Expand all

Employees Management (EXAMPLE)	▼
Claims and suggestions (EXAMPLE)	▼
Security of the facilities (EXAMPLE)	▼
Orders management (EXAMPLE)	▼
Procurement and outsourcing management (EXAMPLE)	▼

Add new data processing

Report generation and export

The reports generated have the character of supporting documents for the implementation of risk management, and in no case substitute or replace the actions to be taken by controllers and processors.

Report of Records of Processing Activities (Art.30 GDPR)

Print preview

html file

doc file

Data Processing Inventory (includes lawfulness)

Print preview

html file

doc file

Extended Report of Records of Processing Activities

html file

doc file

Export data to CSV (Excel, etc)

csv file

Important:

- Remember to save your work in a file with the Save button. When closing the browser or refreshing the page the data is lost.
- Don't forget to make the corresponding backup copies of the file.
- All data processing belong to a single controller

This tool enables the management of an entity's processing operations in the following aspects: management of the Records of Processing Activities, generation of the Inventory of Processing Operations and the minimum bases for initiating risk analysis and management activities within the scope of the GDPR, generation of reports and management and local storage of data. No information or copies are transmitted to or

Main screen showing a data processing expanded info:

Personal Data Processing

Personal data processing are listed below:

Expand all

Employees Management (DATA PROCESSING EXAMPLE, PLEASE DELETE)

Videosurveillance - face recognition (DATA PROCESSING EXAMPLE, PLEASE DELETE)

Data processing name	Videosurveillance - face recognition (DATA PROCESSING EXAMPLE, PLEASE DELETE)
Processing description	Videosurveillance premises perimeter, Fixed cameras, Face recognition for access secure areas
Typical processing in SMEs	Video surveillance-based security
Joint controller	N/A
Controller's representative	N/A
Data Protection Officer	Data Protection Services Consulting (TEST) info@data-protection-sc.com

Personal Data Processing

Lawfulness (1)	Art. 6.1.f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child Security of company main premises
Lawfulness (2)	Art. 9.2. One of the conditions for lifting the prohibition on processing of special categories of personal data is met (Art. 9.1). Specify which condition is met and indicate the supporting documentation
Purposes	Security of persons and building No risk factors specified
Data subjects	all people in company's premises No risk factors specified
Personal data	video, images Risk Factors: <ul style="list-style-type: none">• Biometric data

Intrinsic Risk Assessment

(0.850) High Risk

Residual Risk Assessment

(0.775) Medium Risk

DPIA RECOMMENDED

Edit/Show Data Processing



Risk assessment screen for one of the data processing:

[Back to Data Processing Management](#)

Test Company (PLEASE DELETE ALL TEST PROCESSING) - Data processing 2: Videosurveillance - face recognition (DATA PROCESSING EXAMPLE, PLEASE DELETE)

Purposes **Types of data** Scope Data subjects Techniques Collection Effects Controller Communications Other Security **Risk Management**

Biometric data

- ☐ Fingerprint
- ☒ Facial features
- ☐ Iris
- ☐ Palm veins
- ☐ Voice
- ☐ Ear
- ☐ Gestures
- ☐ Gait
- ☐ Body descriptors of any kind
- ☐ Other

Mitigation

Not Mitigated Mitigated

⚠ Not Mitigated

Genetic data

- ☐ Apply

Mitigation

Not Mitigated Mitigated

Special categories of data or data that allows to infer special categories of data

- ☐ Ethnic origin
- ☐ Racial origin
- ☐ Political opinions
- ☐ Religious convictions
- ☐ Philosophical convictions
- ☐ Trade union membership
- ☐ Health-related data
- ☐ Data concerning sexual life/orientation
- ☐ Other

Mitigation

Not Mitigated Mitigated

Special categories of pseudonymised data

- ☐ Apply

Mitigation

Not Mitigated Mitigated

Risk management summary screen:

[Back to Data Processing Management](#)

Test Company (PLEASE DELETE ALL TEST PROCESSING) - Data processing 2: Videosurveillance - face recognition (DATA PROCESSING EXAMPLE, PLEASE DELETE)

[Purposes](#) [Types of data](#) [Scope](#) [Data subjects](#) [Techniques](#) [Collection](#) [Effects](#) [Controller](#) [Communications](#) [Other](#) [Security](#) [Risk Management](#)

Data Processing risk management : Videosurveillance - face recognition (DATA PROCESSING EXAMPLE, PLEASE DELETE)

04/06/2023

Intrinsic Risk Assessment

⚠️ (0.850) High Risk

Residual Risk Assessment

ℹ️ (0.775) Medium Risk

DPIA RECOMMENDED

Identified risk sources(grouped by category):

Purposes	<ul style="list-style-type: none">No risk factors specified
Types of data	<ul style="list-style-type: none">Biometric data - Mitigation: Not Mitigated <i>Mitigation/control measures</i>
Scope	<ul style="list-style-type: none">No risk factors specified
Data subjects	<ul style="list-style-type: none">No risk factors specified
Techniques	<ul style="list-style-type: none">Video surveillance - Mitigation: Limitedly mitigated <i>Mitigation/control measures</i> - <i>Concept and design</i> : Replace automated processing with manual processing incorporating monitoring and control procedures..
Collection	<ul style="list-style-type: none">No risk factors specified
Effects	<ul style="list-style-type: none">No risk factors specified
Controller	<ul style="list-style-type: none">No risk factors specified
Communications	<ul style="list-style-type: none">No risk factors specified
Other	<ul style="list-style-type: none">No risk factors specified
Security	<ul style="list-style-type: none">No risk factors specified <i>Mitigation/control measures</i> - (ENS mp.com.2) Protection of communications : Confidentiality protection

Mitigation/Control measures menu:

Management procedure to reduce the risk

For each risk factor, you need to select measures that could be taken to manage the risk to the rights and freedoms of data subjects. To assist in your selection, follow the steps below:

The lists of measures that can be selected are neither exhaustive, nor mandatory, nor minimum measures, but illustrative. The controller or processor has to manage the risk by addressing the specific peculiarities of its processing.

Step 1

Mitigation/Control measures associated with certain risk factors

Depending on the selected risk factor, some mitigation measures are shown, which may be common to other risk factors.

[Show measures](#)

Step 2

Personal data breach management and data security measures for the rights and freedoms of natural persons

Specific controls should be put in place to ensure proper detection and management of personal data breaches. To protect data security for the rights and freedoms of individuals, the approach set out in the ENS is recommended, extending to measures to ensure resilience, as well as to prevent failures and errors in data protection safeguards and applications.

[Show measures](#)

Step 3

Organisational, governance and data protection policy Mitigation/Control measures

General measures common to all risk factors. Depending on the level of risk of the processing, these measures will need to be more stringent.

[Show measures](#)

Mitigation/Control measures selection:

Management procedure to reduce the risk

The following is a list of measures and safeguards that could be adopted to manage the risk; it is not exhaustive, neither mandatory nor minimum. The data controller or data processor must manage the risk by addressing the specific peculiarities of its processing.

Select or introduce measures (by default a certain level of mitigation is established, which is also to be reviewed).

Measurements extracted from the guidelines published by AI PID: "Risk management and impact assessment in the processing of personal data"

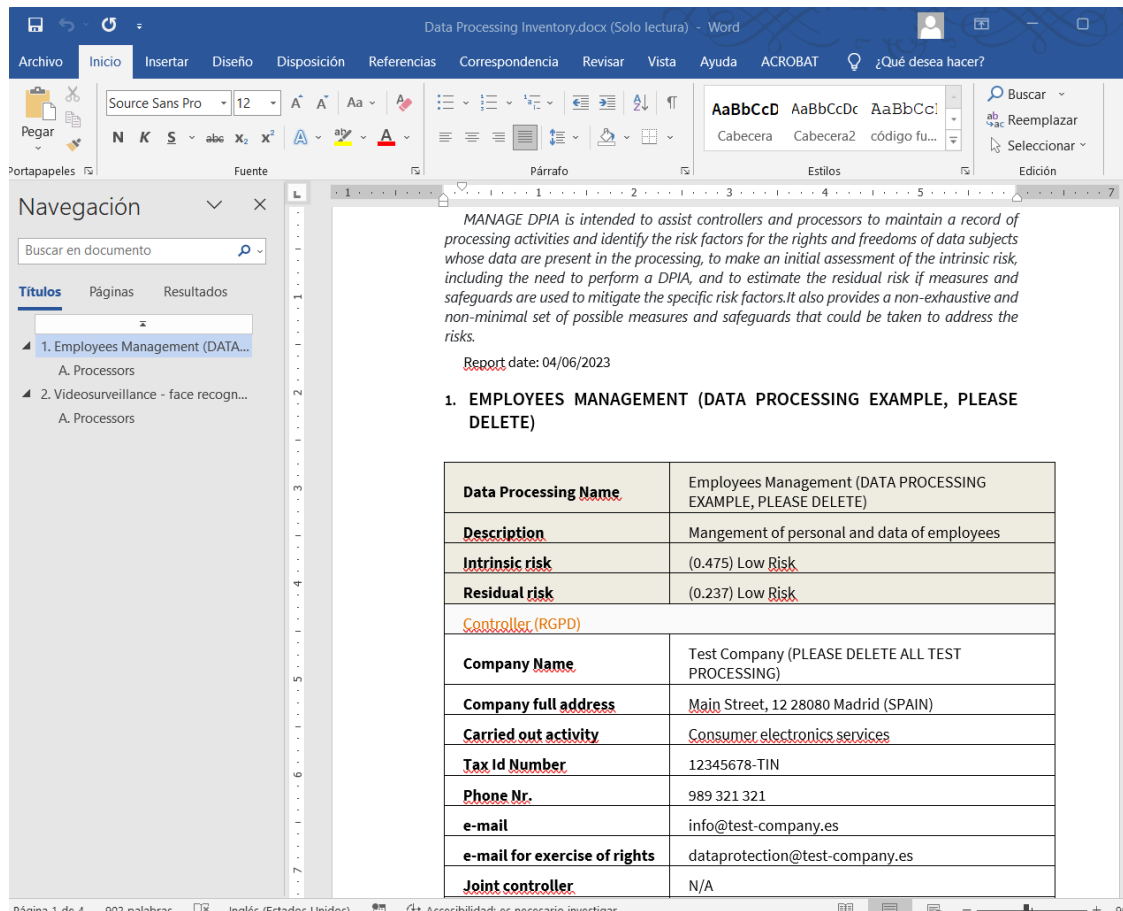
Operation	Description
Video surveillance	Review data processing procedures.
Video surveillance	Change technical choices to implement processing operations by less invasive and/or more mature technologies.
Video surveillance	Switch, in the above sense, to technologies that are more reliable from a data protection point of view, by using for example, the use of PFTs (Privacy Enhanced Technologies).
Video surveillance	Replace automated processing with manual processing incorporating monitoring and control procedures.
Video surveillance	Redesign the procedures for collecting, enriching or generating personal data.
Risk factor 1	Limit the degree to which the processing interacts or is linked to other processing of the same entity.
Observance	Define, within the processing, concrete use cases with disjoint scopes.
Observance Risk factor 1	Limit links or relationships with other controllers' processing.

Other available control and mitigation measures

Operation	Description
-	Change, rearrange or reorganise the phases of processing.
-	Eliminate some phase of processing.

Acceptar

Example of generated report (record of processing activities, word document, html format can be generated as well)



e. Please provide the most relevant link on the authority's website to the initiative, if applicable (The website content does not need to be in English)

This tool can be found here: <https://gestion2.aepd.es/>

English version is available selecting it at the right top of the screen.

f. Please provide any other relevant links that help explain the initiative or its impact or success (e.g. links to news reports or articles):

This tool allows a practical way to implement the first risk methodology for the rights and freedoms of physical person on a personal data processing. This methodology was published by AEPD and includes the management of the accountability principles of GDPR developed by the Spanish DPA in the following resources:

- Privacy risk management principle: [Risk management and DPIA for the rights and freedoms of physical persons](#)
- [List of tables of the guidelines Risk Management and Impact Assessment in the Processing of Personal Data](#)
- [List of the types of data processing that require a DPIA](#)
- Data protection by design principle: [Guideline on Data Protection by Design](#)

- Data protection by default principle:
 - o [Guideline for Data Protection by Default](#)
 - o [List of measures on Data Protection by Default principle](#)
- Security principle for the rights and freedoms for data subjects based on the Spanish [National Security Framework](#)

The Spanish methodology risk for the rights and freedoms of physical persons is becoming a standard implemented in [private](#) and [public](#) tools sectors, this tool implements an holistic view of the obligations of controllers and processors and integrates low risk and high risk personal data processing management in contrast with former tools published by the Spanish DPA.

This tool does not require configuration or other technical resources than just a simple web browser, there are no cloud services neither additional databases are required and no third party is involved in the management of the processing of controllers or processors providing an additional layer of confidentiality for the business and processing activities of controllers and processors of personal data since everything is locally processed in the computer of the user.

This tool will also help controllers and processors to face prior consultation requirements of GDPR article 36 in case the level of risk would remain high after the implementation of measures in the processing since reports provided by this tool will give answer to article 36.3 requirements.

In the end, this is a milestone of a process in which the Spanish DPA has been involved since 2016 as soon as GDPR was publish and is the culmination of the lines of work that were initiated in 2015 in the context of the [strategic plan of the AEPD](#) in which the design of the current [Division of Innovation and Technology](#) was initially outlined becoming nowadays a reference in accountability in the context of privacy and personal data protection after the huge amount of publications and resources published to help data subjects, controllers and processors.