



User Manual

Manage GDPR

April 2024

INDEX

I.	OBJECT AND SCOPE OF MANAGE GDPR TOOL	4
II.	DESCRIPTION AND USE OF THE APPLICATION	4
A.	Start of the Application and General Considerations	5
1.	Menu in the header of the homepage	8
B.	Entering new p personal data or edit an existing one	11
1.	Formatted Data Entry Text Boxes	13
C.	Risk Management: Data Processing Risk Factors and Mitigation Measures	13
1.	Risk management and mitigation measures	15
2.	Result of the assessment and need for DPIA	21
D.	End the session, save data, and exit the application	26
III.	REFERENCES	27

Index of Figures

FIGURE 1	APPLICATION HOME SCREEN WHEN LOADING THE WEB.	5
FIGURE 2	HOME SCREEN WHEN UPLOADING A DATA FILE OR ENTERING SOME DATA PROCESSING	6
FIGURE 3	PROCESSING DATA WHEN EXPANDED IN THE LIST OF PROCESSING	7
FIGURE 4	TYPICAL DATA PROCESSING OF SMES CONSIDERED TO BE LOW RISK FOR WHICH HELP DOCUMENTS ARE PROVIDED	7
FIGURE 5	DOWNLOAD A HELP DOCUMENT AS IT IS A TYPICAL LOW RISK PROCESSING IN SMES	8
FIGURE 6	HOME PAGE HEADER MENU	8
FIGURE 7	DARK MODE	9
FIGURE 8	HELP PANEL	9
FIGURE 9	REPORTS/EXPORT DROP-DOWN MENU.	10
FIGURE 10	PROCESSING DATA FORM	11
FIGURE 11	DATA OF A DATA PROCESSOR	12
FIGURE 12	EXAMPLE OF USING FORMATTED TEXT IN A TEXT FIELD.	13
FIGURE 13	RISK MANAGEMENT SCREEN: PURPOSES	14
FIGURE 14	RISK FACTOR SELECTED. MITIGATION SELECTOR ENABLED.	14
FIGURE 15	MITIGATION SELECTOR VALUES.	15
FIGURE 16	EXAMPLE OF A RISK FACTOR ADDED BY THE USER.	15
FIGURE 17	BUTTON TO DISPLAY MITIGATION ACTION TABLES	16
FIGURE 18	BUTTONS TO SELECT MITIGATION MEASURES.	17
FIGURE 19	ANOTHER MEASURE ADDED BY THE USER FOR THE INDICATED RISK FACTOR.	17
FIGURE 20	SECURITY MEASURES AND DATA BREACHES	19
FIGURE 21	COMMON ORGANISATIONAL AND GOVERNANCE MEASURES.	20
FIGURE 22	SELECTED MEASUREMENT, DIFFERENT BACKGROUND COLOR	20
FIGURE 23	RISK MANAGEMENT, SUMMARY AND RESULTS	22
FIGURE 24	HIGH RISK, RECOMMENDED DPIA	23
FIGURE 25	A MANDATORY DPIA CONDITION IS MET	23
FIGURE 26	SUMMARY TABLE	25
FIGURE 27	HELP FILLING OUT THE SUITABILITY TRIAL	26
FIGURE 28	WARNING WHEN CLOSING THE BROWSER TAB	27

I. OBJECT AND SCOPE OF [MANAGE GDPR TOOL](#)

[MANAGE GDPR](#) is a support resource that does not replace the controller in its decisions related to risk management processes or in any of its decisions related to the purposes and means of the processing carried out or any other aspect of compliance with the regulations on the personal data protection applicable to its processing. Therefore, the tool does not take any of the decisions that correspond to the controller and processor, but is intended as an advisory resource for the risk management and processing related actions of a controller or processor.

The tool [MANAGE GDPR](#) helps controllers and processors to keep a record of processing activities, to identify to a large extent the risk factors for the rights and freedoms of data subjects whose data are present in the processing and to propose to the controller or processor an first assessment of intrinsic risk, including the recommendation or obligation to conduct a DPIA and estimate the residual risk if measures and safeguards are used to mitigate the specific risk factors. In addition, [MANAGE GDPR](#) has the capacity to achieve these objectives with multiple processing operations of the same controller.

The tool works in a web environment, and it is only necessary to have a browser to use it, all processing management is carried out in the user's own browser, with no data being transmitted to the Agency and with total confidentiality. During the work session, the information is stored in the memory of the browser's execution process, which means that all the information is stored on the user's device and the change of URL, closing the tab or browser includes the deletion of the data entered in the tool. However, the information can be stored in a file on the user's computer and retrieved after each session, allowing different versions in different computer files.

In no case does the use of this tool imply the implementation of risk management or a DPIA or compliance with the provisions of the data protection regulations "automatically", but rather a basis on which the controller and processor can rely to guarantee and be able to demonstrate that the processing is in accordance with the provisions of the GDPR. In short, Manage GDPR, in its state of evolution, is the starting point to start risk management.

Consequently, simply obtaining the documents provided by the tool does not imply, in any case, an automatic compliance with the obligations that the GDPR establish for controller for controllers and processors of personal data processing, in particular with regard to the principle of accountability that the GDPR develops in its Chapter IV. These are initial help documents aimed at facilitating the understanding of these obligations and addressing them, initially, in an appropriate manner.

This document guides users through the application interface detailing its functionalities and steps to follow.

II. DESCRIPTION AND USE OF THE APPLICATION

The tool runs in a web browser locally (no data is transmitted over the internet and uses the local storage of the user's browser). It works on any operating system with an up-to-date browser (Windows, Mac OSX, Linux, Android, iOS). It consists of two screens, the Home screen, with the set of data processing, and the risk management screen, specific to a data processing.

The Home screen allows you to add processing by entering detailed information (including that indicated in Art. 30.1 GDPR). It shows the managed data processing, dumps the results

of the risk assessment carried out and allows the generation of reports and the storage and loading of the set of data processing from a file.

The risk assessment screen of a data processing allows you to select the risk factors identified in the processing, the mitigation measures to manage the risk and calculates an assessment of the intrinsic and residual risk, as well as the recommendation or obligation to carry out a DPIA.

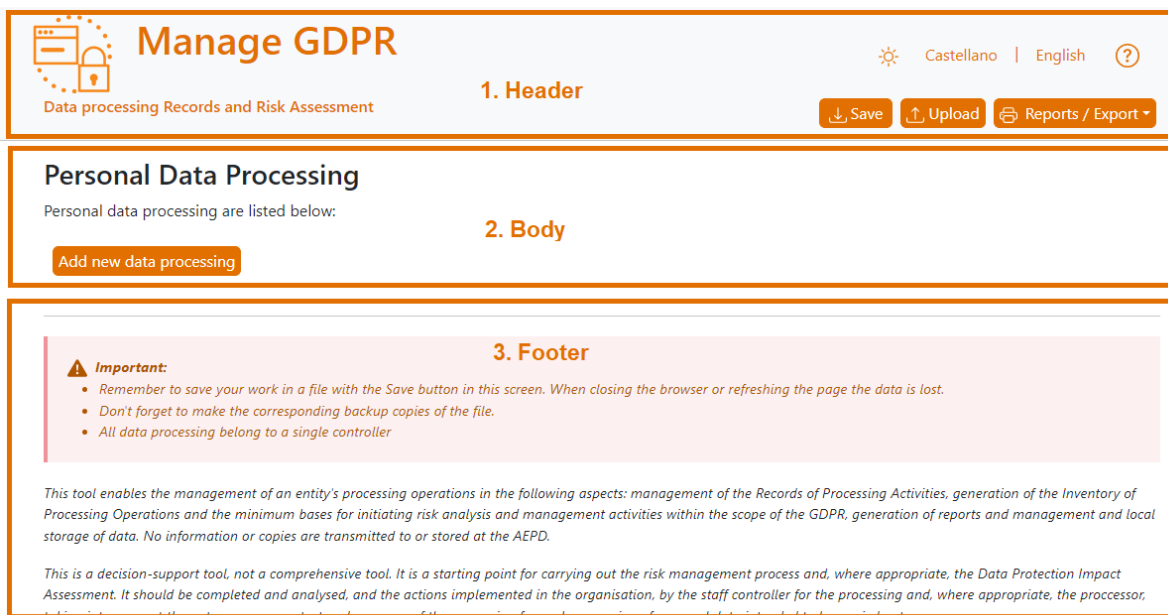
A. START OF THE APPLICATION AND GENERAL CONSIDERATIONS

The application is developed to keep a record of the different processing operations carried out by a single controller. If you w to manage processing by different controllers, then you will have to run the application for each of them and store the data with the tool in different files.

The application is prepared to handle a large number of data processing, but it must be taken into account that it runs in the user's browser and that it is a web application that displays pages with very extensive content, therefore depending on the resources of the user's computer. If there are a considerable number of data processing and they contain very long texts and a large number of risk mitigation measures, i.e. a lot of data, the display of web pages by the browser may be slowed down. Similarly, the generation of reports can also be more time-consuming. In these cases, it is advisable to separate them into different files with fewer data processing.

When the web page loads, the app displays the Home screen without any data processing. Data processing must be generated by adding new processing with the button available for this purpose, or by uploading a data file previously saved with the application.

The home screen is divided into three distinct areas: headboard, body, and foot. The header shows the menus for using the application, the body shows the set of data processing, and the footer shows some considerations to keep in mind.



The screenshot shows the 'Manage GDPR' application interface. It is divided into three main sections:

- 1. Header:** Contains the title 'Manage GDPR', a subtitle 'Data processing Records and Risk Assessment', language options for 'Castellano' and 'English', a help icon, and buttons for 'Save', 'Upload', and 'Reports / Export'.
- 2. Body:** Features the heading 'Personal Data Processing' and the text 'Personal data processing are listed below:'. A prominent orange button labeled 'Add new data processing' is visible.
- 3. Footer:** Includes an 'Important' warning section with three bullet points:
 - Remember to save your work in a file with the Save button in this screen. 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
 Below this, there is a paragraph of explanatory text about the tool's capabilities and a disclaimer stating it is a decision-support tool, not a comprehensive one.

Figure 1 Application Home screen when loading the web.

When some data processing have been added or a data file has been uploaded, the home screen displays the data of the controller and a drop-down list with the set of data processing. The footer shows the options for creating reports (also available in the header menu)



Manage GDPR

☀ Castellano | English ?

Data processing Records and Risk Assessment

↓ Save ↑ Upload 📄 Reports / Export ▾

Data Processing Controller

[...Controller name and contact data...] [...TIN...]
 [...Full Address...]
 [...Phone...] [...email...]
 [...Brief description of activity...]
 data subject rights: [...email_for_exercise_of_rights...]
 [...DPO contact data ...]
(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

Data processing 1	▾
Data processing 2	▾
Data processing 3	▾

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 in this screen. When closing the browser or refreshing the page the data is lost.
- Don't forget to make the corresponding backup copies of the file.

Figure 2 Home screen when uploading a data file or entering some data processing

When one of the data processing is expanded, the details of the processing (the information that has been entered in the form when it has been created or modified) are displayed together with the summary of the risk assessment in a box on the right, where there are also buttons to edit and modify the processing data or to delete it.

[...DPO contact data ...]
 (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](#)

Data processing 1
↑

Data processing name	Data processing 1
Processing description	[...data processing description...]
Controller (GDPR)	
Controller Company name	[...Controller name and contact data...]
Company full address	[...Full Address...]
Carried out activity	[...Brief description of activity...]
Tax Id Number	[...TIN...]
Phone Nr.	[...Phone...]
e-mail	[...email...]
e-mail for exercise of rights	[...email_for_exercise_of_rights...]
Joint controller	
Controller's representative	Representative
Data Protection Officer	[...DPO contact data ...]
Personal Data Processing	
Lawfulness (1)	Art. 6.1.b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract

Intrinsic Risk Assessment

i (0.700) Medium Risk

Residual Risk Assessment

✓ (0.140) Low Risk

Edit/Show Data Processing
🗑️

Figure 3 Processing data when expanded in the list of processing

If the processing has also been indicated as one of the usual low-risk processing in SMEs and Micro-SMEs, the right column of the view will contain the button to download the help document file provided by the tool that will help the controller to adapt to the GDPR the processing of data on customers, potential customers, employees, personnel selection, supplier management and video surveillance.

Typical processing in SMEs

In case the entity is an SME, help documents are provided for the following processing if the risk is low. Please select the one to which this processing applies (only one):

- i [More...](#)
- | | |
|---|--|
| <input type="checkbox"/> Customer service | <input type="checkbox"/> Recruitment of new staff (HR) |
| <input type="checkbox"/> Actions to attract potential customers | <input type="checkbox"/> Supplier management |
| <input type="checkbox"/> Employee Management (HR) | <input type="checkbox"/> Video surveillance-based security |

Figure 4 Typical data processing of SMEs considered to be low risk for which help documents are provided

Intrinsic Risk Assessment
✓ (0.475) Low Risk

Residual Risk Assessment
✓ (0.237) Low Risk

Edit/Show Data Processing

As this **Customer service** data processing is low risk, you can download the informative clauses, data processor contracts and directives for data subjects exercise of rights (tool *Facilita*)

↓ Download document

Figure 5 Download a help document as it is a typical low risk processing in SMEs

1. Menu in the header of the homepage

A two-line menu is displayed at the top of this home page.

☀️ Castellano | English ?

↓ Save ↑ Upload 🖨 Reports / Export ▾

Figure 6 Home Page Header Menu

A sun or moon icon appears at the top to indicate the preferred color mode to display the page (light or dark color mode) when clicked on. The dark color mode inverts the colors

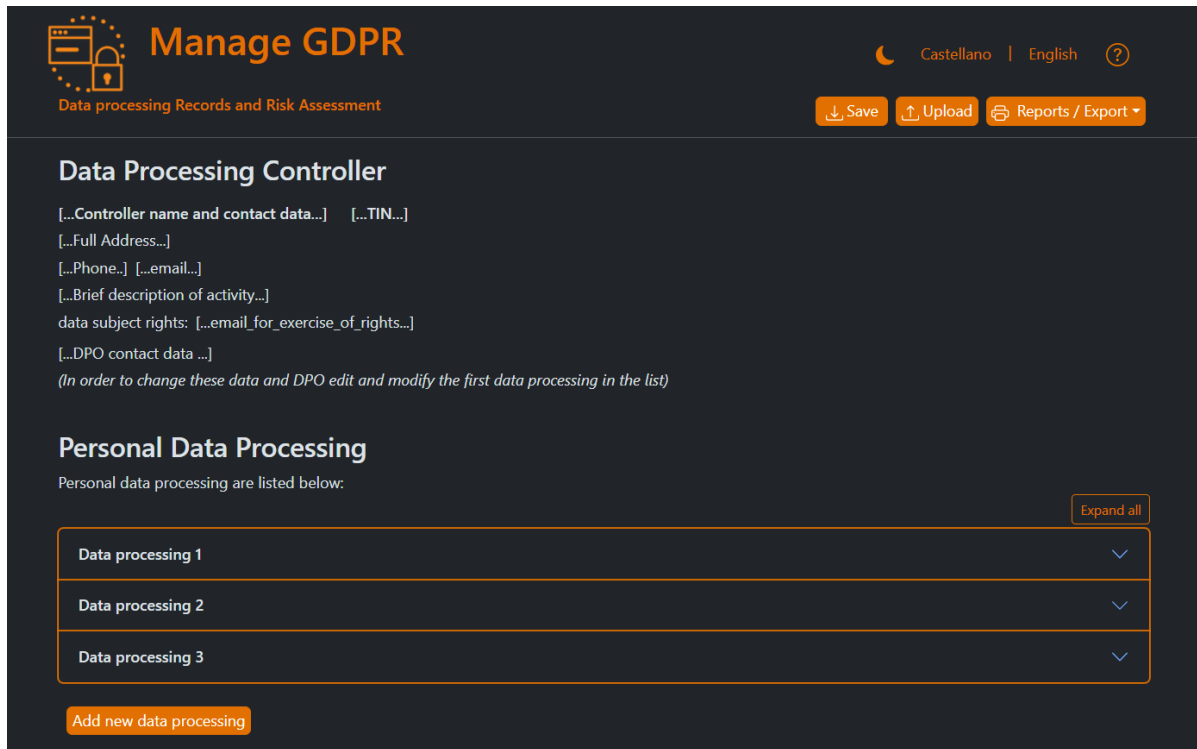


Figure 7 Dark Mode

The next option is the choice of the language displayed, by clicking on the desired one. Finally, the question mark icon shows a side panel with a brief help when you click on it.

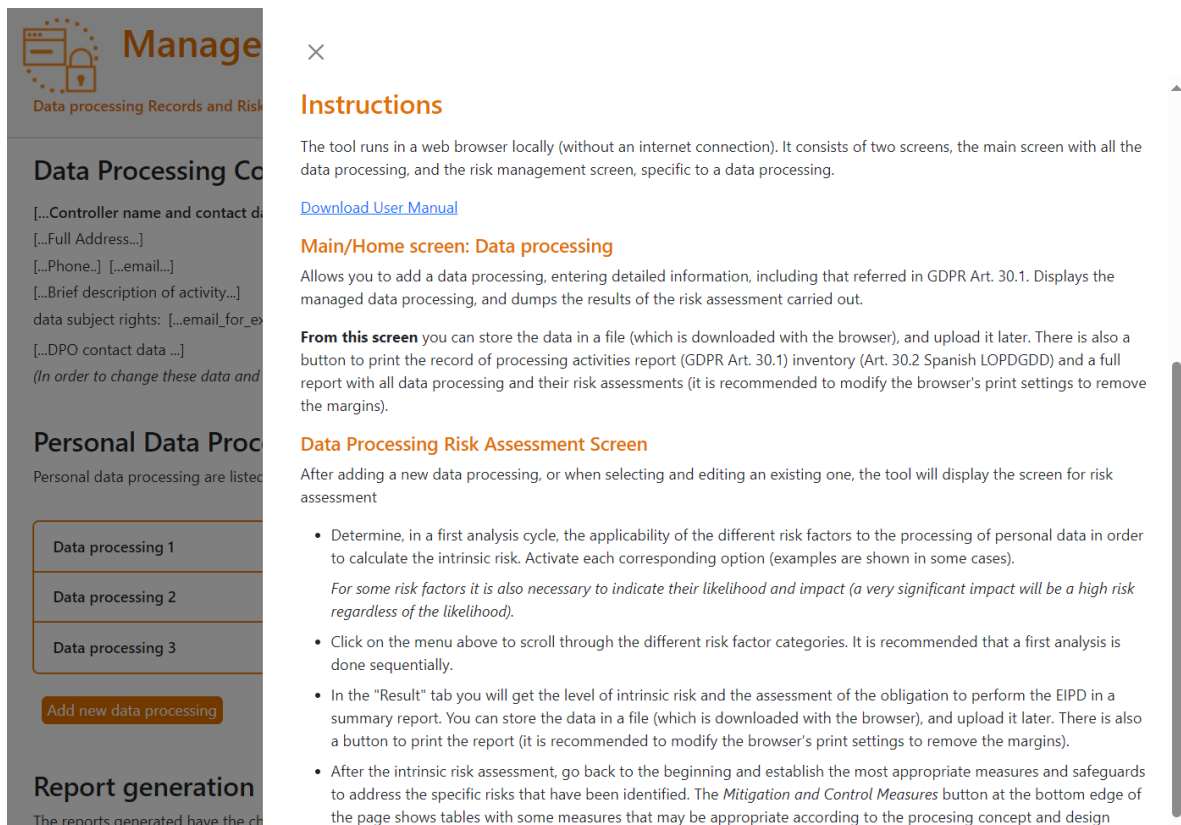


Figure 8 Help Panel

The second line of this menu contains the buttons to save and load data files generated by this application, whose extension will always be ".aepd". Not using this extension will prevent the tool from locating the previously generated files to proceed with their loading or editing.

The **Save** button stores in a file all the data processing and the risk assessment that has been done with the application and are shown on the screen, in the list of data processing. The data is stored in the memory of the user's browser execution process and is written to a text file with a predefined name '*Data_processing.aepd*'. The way to save the file through the browser is by downloading it locally.

The **Upload** button clears all the data and processing that are on the screen and loads into memory and displays on the screen those found in the file that is selected with the file explorer (which must be one previously generated with the application).

The **Reports/Export** button displays a drop-down menu with the different options for generating reports:

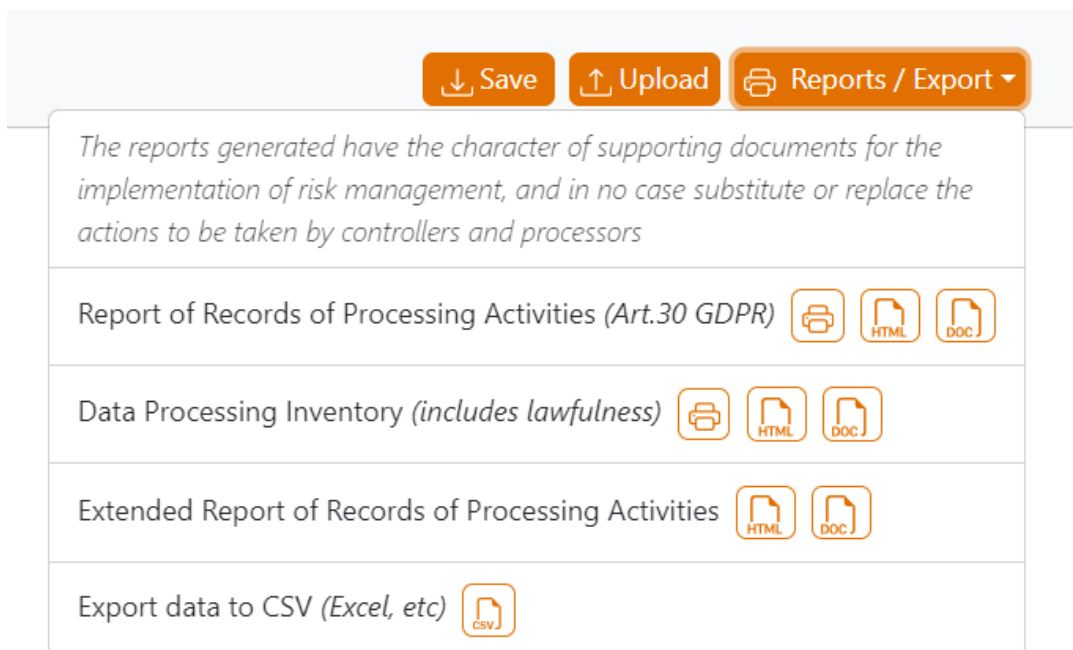


Figure 9 Reports/Export drop-down menu.

There are three types of reports depending on the information they contain. The Record of Processing Activities collects the necessary information for each data processing in order to comply with Art. 30 of the GDPR (data of the controller, purposes, data subjects, etc.). The Data Processing Inventory adds to the previous one the information corresponding to the legal basis of the processing to be used for transparency purposes and, finally, the extended report that incorporates for each data processing defined by the controller, the information from the Risk Assessment.

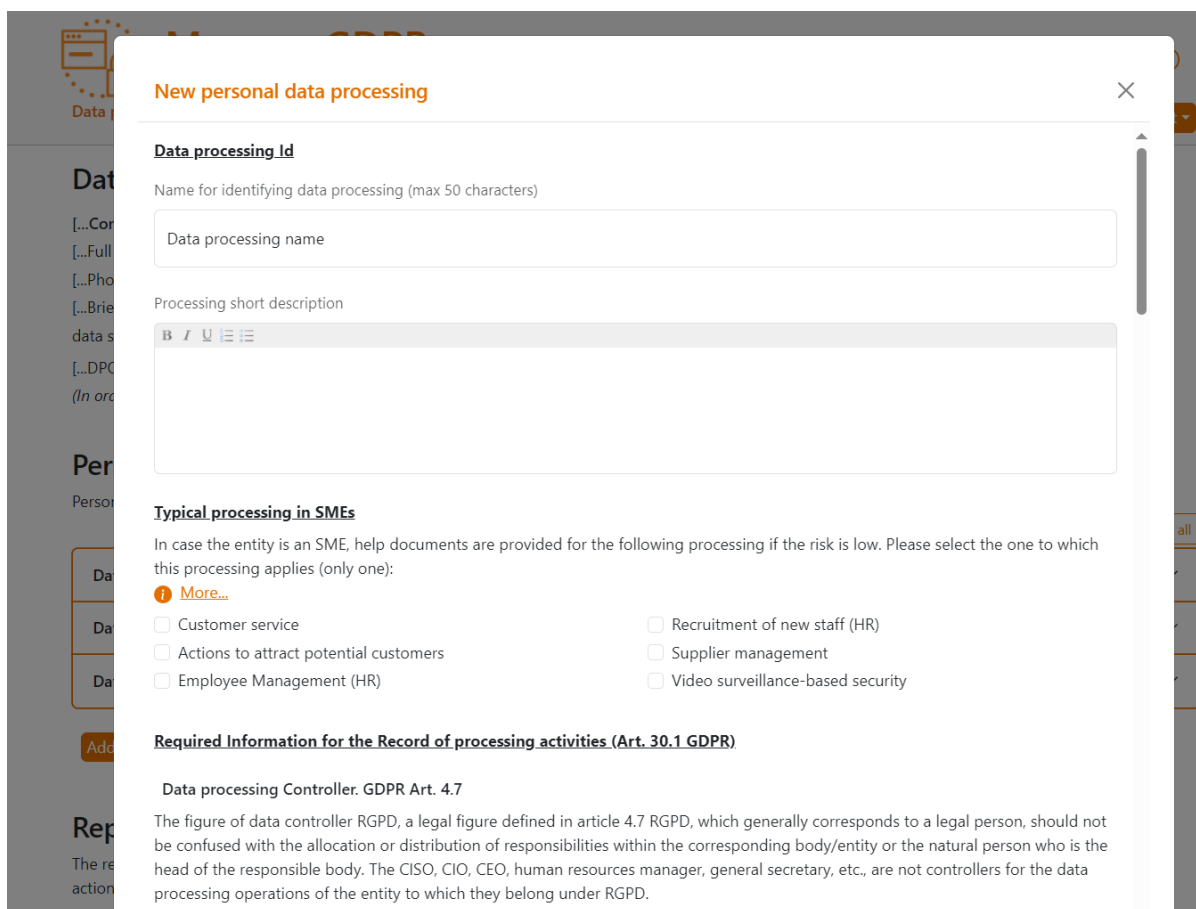
All data can be downloaded in table format (CSV) so that they can be processed with spreadsheet applications.

The reports can be obtained using the browser's print view (printer icon, which will require printing to be configured with the browser print options); in HTML format, which allows the browser view to be stored in a file; in Word/Libreoffice document format. By clicking on each icon, the file with the corresponding report is generated and subsequently downloaded locally. The names of the files with the reports are predefined by the application.

As indicated at the beginning of this chapter, the generation of reports, in particular extended reports, may not be immediate or may take some time depending on the number of data processing and the data and information they contain. Keep in mind that all information is processed on the user's device and, therefore, the agility with which it processes will depend on the volume of information that needs to be processed by the device, as well as the specific characteristics of each device.

B. ENTERING NEW P PERSONAL DATA OR EDIT AN EXISTING ONE

By clicking on the *Add new data processing* button at the end of the processing list, or the *Edit/View Processing* button when one is expanded in the list, a form opens on the screen to enter or modify all relevant data and processing details. Some of the fields are required and others are optional (a warning is displayed if a required field is not filled in).



New personal data processing

Data processing Id
Name for identifying data processing (max 50 characters)

Data processing name

Processing short description

Typical processing in SMEs
In case the entity is an SME, help documents are provided for the following processing if the risk is low. Please select the one to which this processing applies (only one):

[More...](#)

Customer service
 Recruitment of new staff (HR)

Actions to attract potential customers
 Supplier management

Employee Management (HR)
 Video surveillance-based security

Required Information for the Record of processing activities (Art. 30.1 GDPR)

Data processing Controller. GDPR Art. 4.7

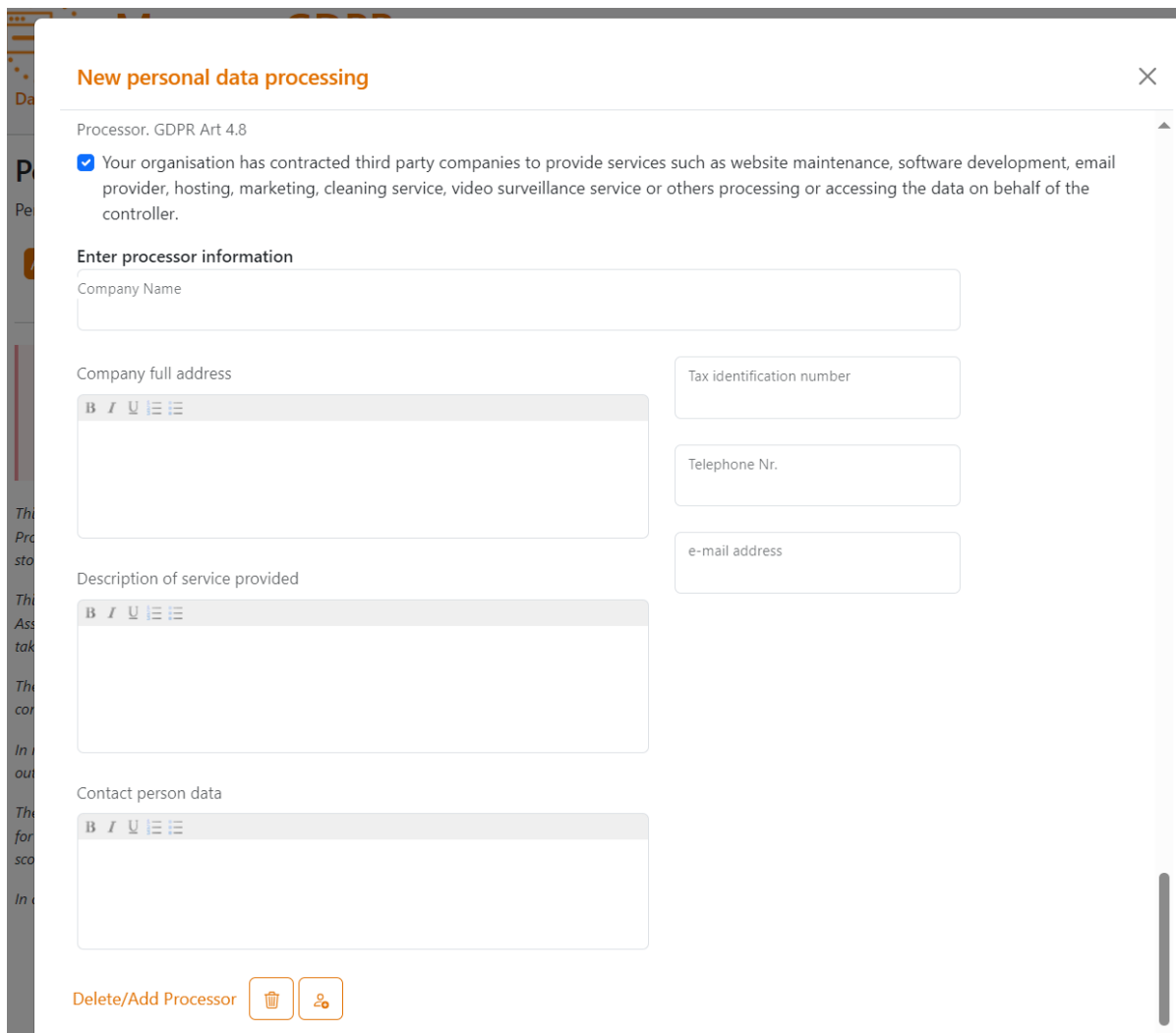
The figure of data controller RGPD, a legal figure defined in article 4.7 RGPD, which generally corresponds to a legal person, should not be confused with the allocation or distribution of responsibilities within the corresponding body/entity or the natural person who is the head of the responsible body. The CISO, CIO, CEO, human resources manager, general secretary, etc., are not controllers for the data processing operations of the entity to which they belong under RGPD.

Figure 10 Processing Data Form

The form distinguishes the following types of data and details to describe a data processing:

- **Identification of the processing:** Name and description
- **Low-risk processing typical of SMEs:** some low-risk processing that are common in SMEs are contemplated. When marking one of them, the tool provides a help document, which replaces the help document that was obtained with the FACILITA GDPR tool. The download of the document is enabled on the home page when the processing is expanded and displayed.

- Information required for the Record of Processing Activities (Art. 30.1 GDPR):**
 - Data of the data controller, representative, joint controller and DPO. The contact data of the controller and the DPO are only filled in or modified in the first processing, as they are common to the rest of the processing (managed in a session or in an uploaded/saved file)
 - Lawfulness of the processing (legal basis and its justification)
 - Details of the processing: purposes, categories of data subjects, personal data and recipients, information on international transfers, time limits for data erasure and general description of security measures.
- Other data:** management or internal unit responsible for the processing, information on data processors and other additional information deemed necessary. By ticking the box for the existence of data processors, fields are displayed to include their data, together with buttons to add a new processor or delete the one entered.



New personal data processing ×

Processor. GDPR Art 4.8

Your organisation has contracted third party companies to provide services such as website maintenance, software development, email provider, hosting, marketing, cleaning service, video surveillance service or others processing or accessing the data on behalf of the controller.

Enter processor information

Company Name

Company full address

Tax identification number

Telephone Nr.

e-mail address

Description of service provided

Contact person data

Delete/Add Processor

Figure 11 Data of a Data Processor

Once the form fields have been filled in (those required that have not been completed are notified), it is necessary to click on the *Save changes and Open risk management* button so that the processing is stored in the browser's execution memory. Once stored, the Risk Management screen opens for processing, explained in section C.

1. Formatted Data Entry Text Boxes

Input text boxes allow you to add text with some formatting options: bold, underline, italics (can be combined), and simple lists (nested lists are not allowed).

The use is very intuitive and it is enough to press the buttons at the top to activate or deactivate each option.

While it is possible to copy and paste text from word processors into the tool's form input fields, and get a correct appearance in the application, formatting modifiers that are not visible to the user are actually also being copied, which can lead to problems and text errors when generating Word/LibreOffice reports. However, the application filters out some modifiers, but cannot be sure to completely avoid the possibility of errors in the generation of such reports.

The size of the text fields is limited to a maximum number of characters, so if it is exceeded, no more text can be included or it will be cut off.

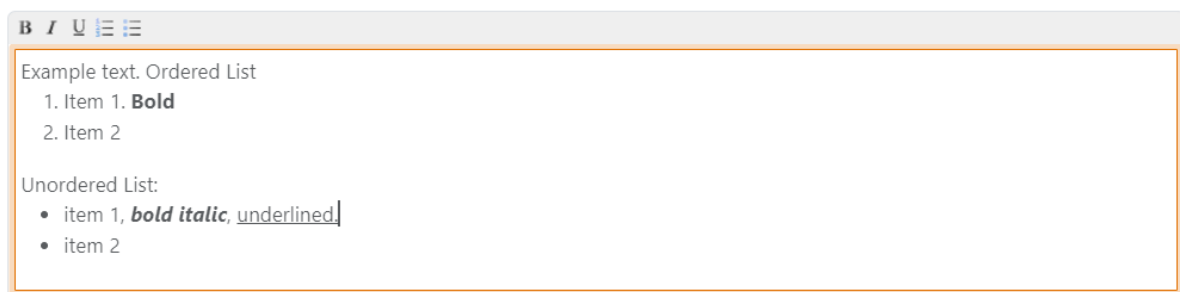


Figure 12 Example of using formatted text in a text field.

C. RISK MANAGEMENT: DATA PROCESSING RISK FACTORS AND MITIGATION MEASURES

One of the main objectives of this tool is to advise the data controller and data processor in the process of managing the risk to rights and freedoms, and as a result of the same process, the recommendation or obligation to carry out an DPIA is proposed to the data controller and data processor. To this end, after saving the data in the form for entering or editing a processing operation, a new screen opens for this purpose.

The screen is divided into two parts, header and body.

The header shows the controller name and the name identifying the processing and a menu with the different categories of risk factors that are contemplated, and the body shows where the identification of risk factors is carried out according to the selected category.

On the right side of the header, you will find the options for changing light/dark mode, Spanish/English language, help panel and a button to return to the home screen of the application with the list of data processing. When the home button is clicked, the risk management data that has been selected and modified is stored in the browser's execution memory.

The body of the page shows the different risk factors for the category selected in the header menu with some examples (including the possibility of adding other examples that are not covered and are considered the same risk factor).

The selectors allow you to indicate those risk factors that are applicable to the processing being managed. The risk values are predetermined by the tool, in some cases it is also necessary to indicate their probability and impact to determine them, that is, the tool suggests an assessment that can be altered by the person in charge through the mitigation slider and

based on their criteria as having detailed knowledge of the nature, the scope, context and purposes of the processing.

Manage GDPR 1. Header

Castellano | English

[...Controller name and contact data...] - Data processing 1: Data processing 1

Home

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

2. Body

Operations related to the purposes of processing

Risk factors arising from the stated purpose of the processing and other purposes linked to the main purpose.

Risk Factor	Mitigation
Profiling <input type="radio"/> Creating profiles <input type="radio"/> Use of profiles <input type="radio"/> Classification of individuals <input type="radio"/> Targeting of products/services to individuals or groups <input type="radio"/> Behavioral analysis (evaluation and rating of emotions, moods, habits, preferences, etc.) <input type="radio"/> Other	Not Mitigated Mitigated <input type="range" value="0"/>
Assessment of subjects <input type="radio"/> Valuation <input type="radio"/> Scoring <input type="radio"/> Other	Not Mitigated Mitigated <input type="range" value="0"/>
Prediction <input type="radio"/> Inference of new personal data <input type="radio"/> Other	Not Mitigated Mitigated <input type="range" value="0"/>
Employee control <input type="radio"/> Employee evaluation <input type="radio"/> Job observation <input type="radio"/> Workplace monitoring	Not Mitigated Mitigated <input type="range" value="0"/>

Figure 13 Risk Management Screen: Purposes

When a risk factor is selected, it is considered applicable to the processing. The mitigation slider is enabled (with an unmitigated default value). This slider can always be moved by the user through the different values depending on the analysis that has been performed. However, the tool moves it automatically when mitigation measures are selected.

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

Unique identifiers

- IP
- MAC
- IMSI or IMEI
- Device ID
- Phone N.
- DNI, NIE, Passport No. or equivalent
- Social security number
- Vehicle registration number
- Credit card number
- UID
- Other

Mitigation

Not Mitigated | Mitigated

⚠ Not Mitigated

Figure 14 Risk factor selected. Mitigation selector enabled.

The possible values that the application considers in relation to the mitigation factor are those indicated in the following figure: *Not mitigated*, *Limitedly mitigated*, *Significantly mitigated*, and *Fully mitigated*.

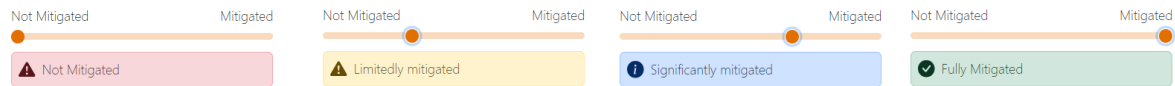


Figure 15 Mitigation selector values.

The tool allows you to add other risk factors that are not covered, *Other tab*, for which it is necessary to indicate the probability and impact by means of sliding selectors in order to calculate the risk (maximum when the probability is very high and the impact very significant, and minimum when it is unlikely and with very limited impact), as shown as an example in the following figure:

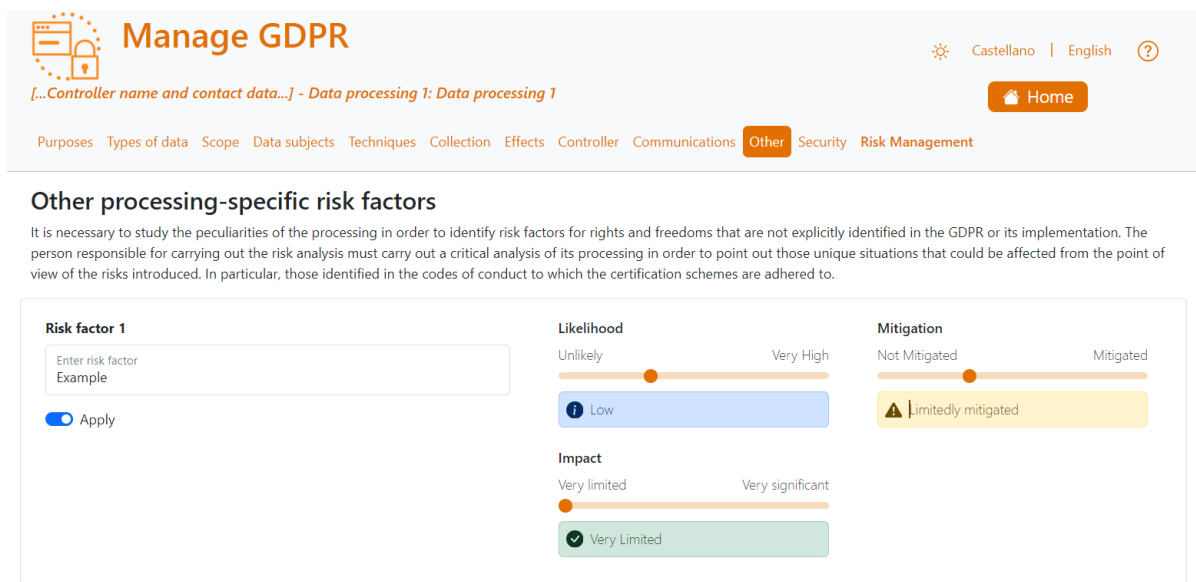


Figure 16 Example of a risk factor added by the user.

The first phase of risk management involves selecting each category of risk factor from the menu and indicating those that are applicable to the processing, and then proceeding with the risk mitigation and management phase, as described in the next section.

The risk factors displayed in this tool are not exhaustive, but minimal, and the controller must identify those that are specific to the processing and include them in its assessment taking into account the nature, scope or scope, context and specific purposes of the processing of personal data.

1. Risk management and mitigation measures

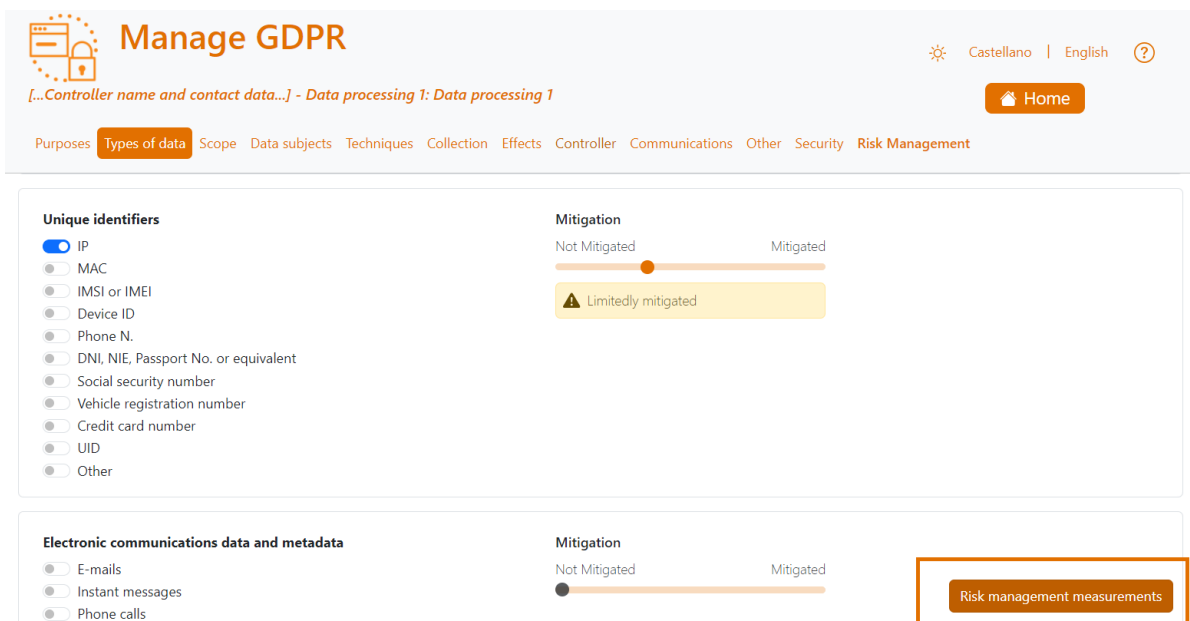
The tool proposes some measures to manage the risks of processing. Different measures associated with the different risk factors that have been selected are proposed, which may be common to several risk factors. It is also possible to add new user-defined measurements.

The measures proposed by the tool are classified into the following dimensions:

- a) **Concept and design of the processing and Data protection by design:** Associated with the processing operations, therefore, to the categories in the top menu *Purposes, Types of data, Scope, Data Subjects, Techniques, Collection, Effects, Controllers, Communications and Others*.
- b) **Security, failures, errors and data breach management:** For security measures, the measures of the Spanish National Security Scheme (ENS) are recommended as a guide (making the ENS category correspond to the level of risk of the processing). It should be noted that, even if risk factors are not selected from the *Security* menu, security and data breach management measures must be established.
- c) **Governance measures and data protection policies:** set of measures that could be implemented when deploying data protection policies as part of the governance of the processing (measures common to those specific to the processing and those established as part of the governance of the organization)

The selection of measures can be done in two ways:

1. On each screen corresponding to the top menu with the categories of risk factors, use the *Measures to manage risk* button at the bottom right edge of the page. A table will be shown with the measurements of dimension **a)** defined in the previous paragraph and dimension **b)** in the risk factor category *Security*.



The screenshot shows the 'Manage GDPR' interface. At the top, there is a navigation bar with 'Types of data' selected. Below it, a breadcrumb trail shows 'Data processing 1: Data processing 1'. A 'Home' button is visible. The main content area is divided into two sections:

- Unique identifiers:** A list of identifiers with checkboxes: IP (checked), MAC, IMSI or IMEI, Device ID, Phone N., DNI, NIE, Passport No. or equivalent, Social security number, Vehicle registration number, Credit card number, UID, and Other. To the right, a 'Mitigation' slider is positioned between 'Not Mitigated' and 'Mitigated', with a yellow box indicating 'Limitedly mitigated'.
- Electronic communications data and metadata:** A list of data types with checkboxes: E-mails, Instant messages, and Phone calls. To the right, a 'Mitigation' slider is positioned between 'Not Mitigated' and 'Mitigated'.

A 'Risk management measurements' button is highlighted with a red box in the bottom right corner of the interface.

Figure 17 Button to display mitigation action tables

2. On the screen displayed when clicking the top menu *Risk management*, where you can select the measures corresponding to the three dimensions **a)**, **b)** and **c)** defined above. It is located after the processing summary table:

Manage GDPR Castellano | English

[...Controller name and contact data...] - Data processing 1: Data processing 1

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

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](#)

Figure 18 Buttons to select mitigation measures.

When you click on the Measures to manage risk button, in any of the above cases, a table is displayed, with some differences depending on whether it is dimensions **a)**, **b)** and **c)**.

a) Concept and design of the processing and Data Protection by design:

The pop-up window displayed contains three distinct parts:

The first presents a table with the mitigation or risk management measures that the tool provides by default for the risk factors (processing operations) that have been selected.

The second shows a table with the rest of the measures provided by the tool, associated by default with other risk factors not selected, but which the data controller may also consider appropriate.

Finally, for each risk factor that has been selected, the possibility of adding new measures is offered. You need to press the *Add* button to save it (you can edit or delete it later)

Other measures implemented:

Unique identifiers

Enter control/mitigation measure for: Unique identifiers [Add](#)

Figure 19 Another measure added by the user for the indicated risk factor.

The tables have two columns, risk factor (processing operation) and description of the measures, in alphabetical order and with a search box.

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 AEPD "[Risk management and impact assessment in the processing of personal data](#)"

Operation	Description	Search...
Unique identifiers	Early anonymization of data	
Unique identifiers	Apply other privacy techniques by design in the processing of personal data	
Unique identifiers	Apply differential privacy techniques in access to personal data	

Other available control and mitigation measures

Operation	Description	Search...
Collection	Cancel early data in processing	
Collection	Give real-time transparency to the interested party about the data processed	
Collection	Reduce the granularity of the data accessed so that information is stored that is the result of a processing of the input data.	
Collection	Reduce the granularity of the data accessed so that information is provided that is the result of the evaluation.	

Other measures implemented:

Unique identifiers

Add

OK

b) Security, Failures, Errors and Data Breach Management:

These types of measures are always necessary, even if no risk factor is selected from the *Security* category. That's why the table shown contains all the measurements available by the tool. If any of the Safety risk factors have been selected as applicable to the processing, in a similar way to case a) above, the tool will offer the possibility of adding new measures.

The tables have four columns, depending on the source document, the type of measure, the ENS reference when applicable, and the description of the measurements, in alphabetical order and with a search box.

Mangement 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 have been extracted from the guidelines published by AEPD "[Risk management and impact assessment in the processing of personal data](#)", "[Guidelines for massive data breach in public sector bodies](#)", and "[Spanish National Security Framework \(ENS\)](#)".

NOTE: In processing operations that are not subject to the obligation of the ENS, the necessary measures must be implemented to manage the level of risk of the assets necessary to support the processing in each of its phases. It is recommended to use at least the measures indicated in the ENS for the security category of the system equivalent to the level of risk of the processing obtained with this tool, together with the control measures to ensure the detection and management of personal data breaches.

Source	Type	Ref.	Description	Q Search...
ENS	Protection Measures	ENS mp.s.3	Protection of services : Protection of web browsing	
ENS	Protection Measures	ENS mp.s.4	Protection of services : Denial of service protection	
Risk Management Guidelines	Management of Personal Data Breaches		Contingency plans for a personal data breach.	
Risk Management Guidelines	Management of Personal Data Breaches		Establishment of technical resources for the automatic detection of personal data breaches.	
Risk Management Guidelines	Management of Personal Data Breaches		Incident management tools adapted to the requirements of the GDPR.	
Risk Management Guidelines	Management of Personal Data Breaches		Procedures for the identification of essential resources to ensure data subjects complete communication	

Other measures implemented:

OK

Figure 20 Security Measures and Data Breaches

c) Governance measures and data protection policies:

These measures are general and common to the organization for all processing, that is why the selection is enabled only when the first processing is being managed from the list of processing on the Home page. The table is displayed only in the *Risk Management* top menu.

The table has two columns, with the type and description of the measurements, in alphabetical order and with a search box. It also offers the option to add new measurements by the user.

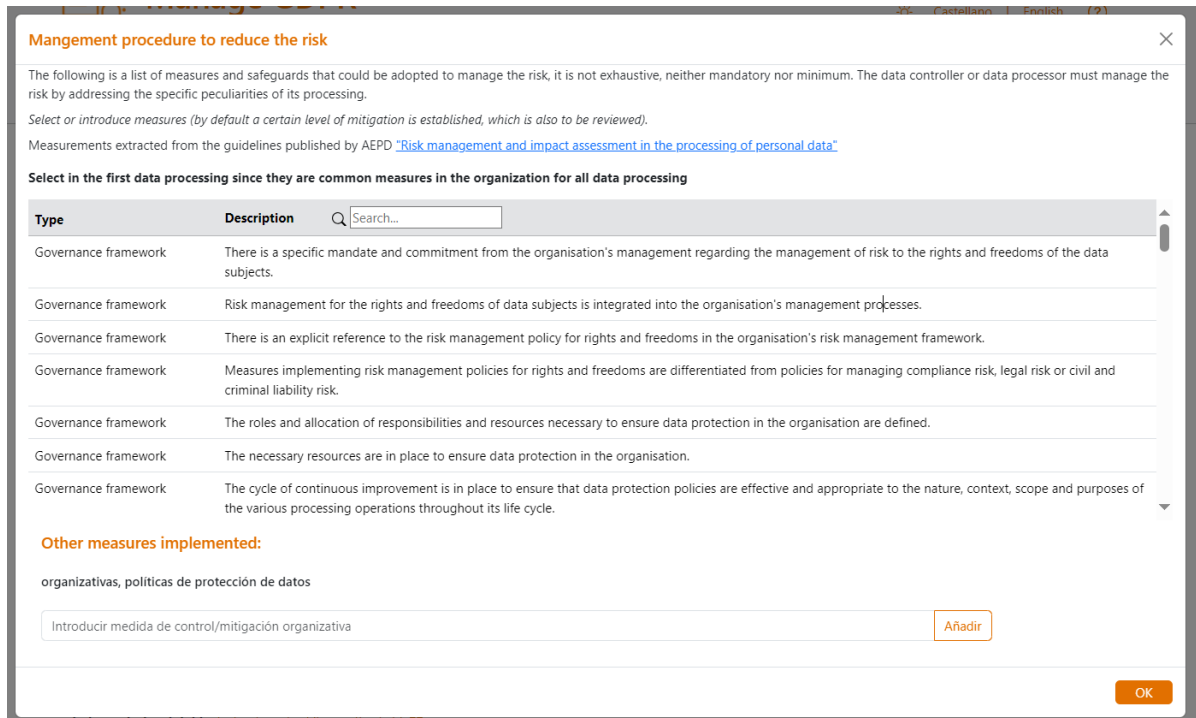


Figure 21 Common organisational and governance measures.

To select a measurement, simply click on the row of the table, changing the background color of the row (to deselect it, simply click again with the mouse). When selecting measures in the proposed tables, the tool considers a default mitigation level (automatically moving the mitigation sliders), although the controller has to manage it by addressing the specific peculiarities of their processing.

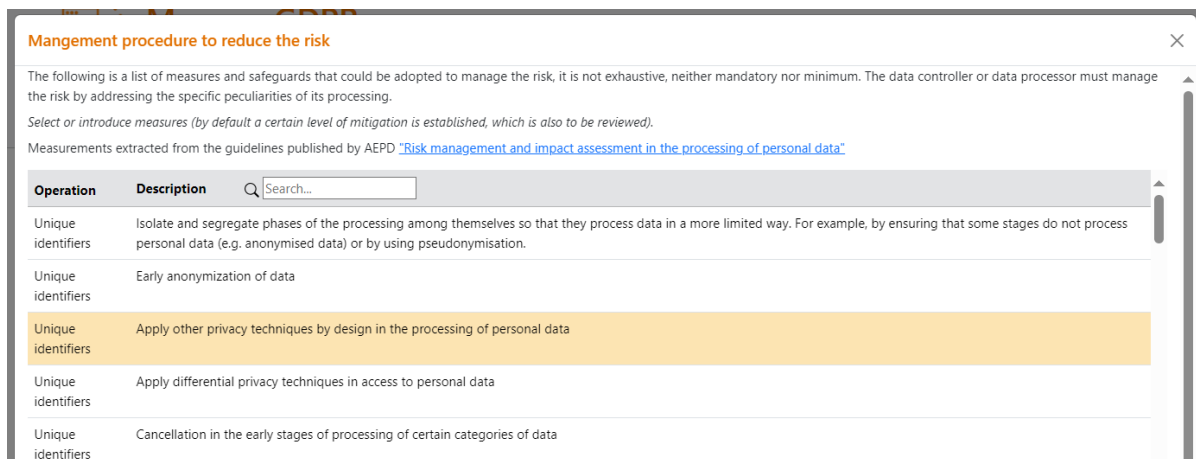


Figure 22 Selected measurement, different background color

When you close the pop-up window or press the OK button (top right and bottom right corner respectively), the selected and added mitigation measures are saved in the browser's execution memory and the relevant Risk Management calculations are performed.

The assessment of the risk level for each factor carried out by the tool, as well as the final risk level calculation, is of a general nature and represents a minimum assessment that,

where appropriate, will have to be adjusted by the controller to determine the risk level of the processing accurately.

2. Result of the assessment and need for DPIA

The top *Risk Management* menu shows a large page with three distinct parts:

- Risk assessment and need for DPIA, summary of identified risk factors and measures applied. The need for DPIA is assessed according to the criteria set out in the GDPR, EDPB and AEPD (Art. 35 GDPR)
- Selection of mitigation measures associated with risk factors, security and data breaches, organizational, governance and data protection policies (already seen in the previous point)
- Assessment of the necessity and proportionality of processing. Fields are shown to be filled in with the corresponding judgments of suitability, necessity and proportionality. This data is saved to the browser's local storage when you press the *Home* button.

Manage GDPR

[...Controller name and contact data...] - Data processing 1: Data processing 1

Castellano | English

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

Data Processing risk management : Data processing 1

26/04/2024

Intrinsic Risk Assessment

(0.475) Low Risk

Residual Risk Assessment

(0.237) Low Risk

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"> Unique identifiers - Mitigation: Limitedly mitigated <p>Mitigation/control measures</p> <ul style="list-style-type: none"> - Apply other privacy techniques by design in the processing of personal data
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"> No risk factors specified
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"> Example - Impact: Very Limited - Likelihood: Low - Mitigation: Limitedly mitigated <p>Mitigation/control measures</p>
Security	<ul style="list-style-type: none"> No risk factors specified <p>Mitigation/control measures</p> <ul style="list-style-type: none"> - (ENS org.3) Security Procedures

Other mitigation/control measures for risk factors

- Restricted access to data to determine solvency
- Restricted access to data that allows financial information to be deduced
- Change in the previous sense by technologies with greater reliability from the point of view of data protection, resorting for example to the use of PEVs (Privacy Enhanced Technologies).

Organisational mitigation measures, governance and data protection policies

- Policies embedded in procedures: Included in the procurement procedures for products, systems or services that are to implement operations within the processing activity are the requirement for information and guarantees to ensure and be able to demonstrate that such processing complies with the GDPR.

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](#)

Assessment of the necessity and proportionality of the processing (DPIA)

GDPR Art. 35.7.b regarding DPIA, requires an assessment of the necessity and proportionality of the processing operations, which according to EDPS guidelines translates into a weighting based on three criteria

Note: Filling in the fields below, as well as the use of this tool, does not imply that the DPIA has been completed.

Judgment of suitability [Instructions for filling in this field](#)

Judgement of necessity [Instructions for filling in this field](#)

Judgement of proportionality in the strict sense [Instructions for filling in this field](#)

once the risk assessment for this data processing has been completed, return to the home screen (processing management) where you can generate reports and save the data in a file.

Figure 23 Risk Management, Summary and Results

The risk assessment shows the results of the calculation of the intrinsic risk of the processing, according to the selected risk factors, and the residual risk, according to the selected mitigation measures. If one of the mandatory conditions for carrying out a DPIA is met, it is indicated, as well as the recommendation of DPIA if the risk is high.

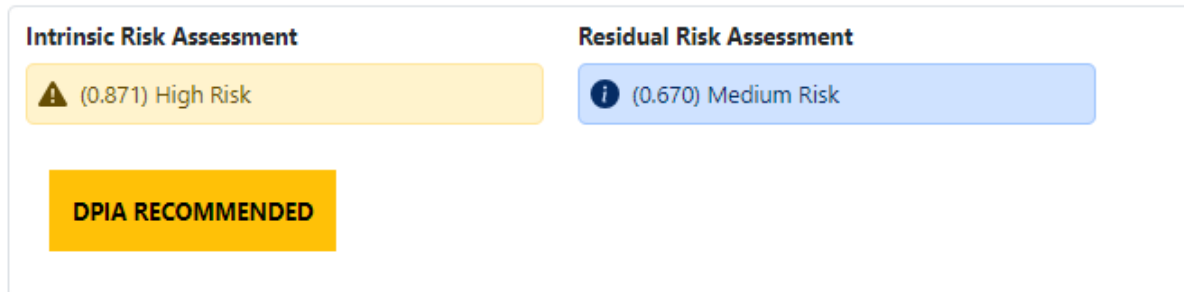


Figure 24 High Risk, Recommended DPIA



Figure 25 A mandatory DPIA condition is met

The summary table shows the risk factors identified by category (the category is shown with a different colored background depending on whether mitigation measures have been implemented or not) together with the provided or additional measures that have been entered for a risk factor in that category.

Alternative measures that have been selected, i.e. those that the tool does not assign by default to a risk factor but has been selected by the controller, are displayed at the end of the table, along with common organizational and governance measures.

The following figure shows a (random) example where the described can be seen:



Manage GDPR Castellano | English

[...Controller name and contact data...] - Data processing 1: Data processing 1

[Home](#) [Risk Management](#)

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

Data Processing risk management : Data processing 1

26/04/2024

Intrinsic Risk Assessment 0.1779 Medium Risk

Residual Risk Assessment 0.5303 Medium Risk

Identified risk sources (grouped by category):

Purposes	• No risk factors specified
Types of data	• No risk factors specified
Scope	<ul style="list-style-type: none"> • Systematic - Mitigation: Limitedly mitigated Mitigation/control measures: <ul style="list-style-type: none"> - Isolate and segregate phases of the processing among themselves so that they process data in a more limited way. For example, by ensuring that some stages do not process personal data (e.g. anonymised data) or by using pseudonymisation. - Eliminate some phase of processing. - Limit the number of participants in the processing - Limit in the conception of the processing the time in which the processing treats data of the same subjects.
Data subjects	<ul style="list-style-type: none"> • Old people - Mitigation: Not Mitigated Mitigation/control measures
Techniques	• No risk factors specified
Collection	• No risk factors specified
Effects	• No risk factors specified
Controller	• No risk factors specified
Communications	• No risk factors specified
Other	• No risk factors specified
Security	<ul style="list-style-type: none"> • No risk factors specified Mitigation/control measures: <ul style="list-style-type: none"> - (ENI org.1) Security Policy - (ENI org.2) Security Regulations

Other mitigation/control measures for risk factors

- Restricted access to data to determine solvency
- Restricted access to data that allows financial information to be deduced
- Change in the previous sense by technologies with greater reliability from the point of view of data protection, resorting for example to the use of PETs (Privacy Enhanced Technologies).
- Cancellation in the early stages of processing of certain categories of data
- Early deletion of data

Organisational mitigation measures, governance and data protection policies

- Governance framework: There is a specific mandate and commitment from the organisation's management regarding the management of risk to the rights and freedoms of the data subjects.
- Governance framework: Risk management for the rights and freedoms of data subjects is integrated into the organisation's management processes.
- Policies embedded in procedures: included in the procurement procedures for products, systems or services that are to implement operations within the processing activity are the requirement for information and guarantees to ensure and be able to demonstrate that such processing complies with the GDPR.

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](#)

Assessment of the necessity and proportionality of the processing (DPIA)

GDPR Art. 35.7b regarding DPIA, requires an assessment of the necessity and proportionality of the processing operations, which according to EDPS guidelines translates into a weighting based on three criteria

Note: Filling in the fields below, as well as the use of this tool, does not imply that the DPIA has been completed.

Judgment of suitability [Instructions for filling in this field](#)

Judgment of necessity [Instructions for filling in this field](#)

Judgment of proportionality in the strict sense [Instructions for filling in this field](#)

once the risk assessment for this data processing has been completed, return to the home screen (processing management) where you can generate reports and save the data in a file.



Manage GDPR

Castellano | English

[...Controller name and contact data...] - Data processing 1: Data processing 1

Home

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

Data Processing risk management : Data processing 1

26/04/2024

Intrinsic Risk Assessment ⓘ (0.779) Medium Risk	Residual Risk Assessment ⓘ (0.500) Medium Risk
---	--

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"> No risk factors specified
Scope	<ul style="list-style-type: none"> Systematic - Mitigation: Limitedly mitigated <p><i>Mitigation/control measures</i></p> <ul style="list-style-type: none"> - Isolate and segregate phases of the processing among themselves so that they process data in a more limited way. For example, by ensuring that some stages do not process personal data (e.g. anonymised data) or by using pseudonymisation. - Eliminate some phase of processing. - Limit the number of participants in the processing - Limit in the conception of the processing the time in which the processing treats data of the same subjects.
Data subjects	<ul style="list-style-type: none"> Old people - Mitigation: Not Mitigated <p><i>Mitigation/control measures</i></p>
Techniques	<ul style="list-style-type: none"> No risk factors specified
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 <p><i>Mitigation/control measures</i></p> <ul style="list-style-type: none"> - (ENS org.1) Security Policy - (ENS org.2) Security Regulations

Other mitigation/control measures for risk factors

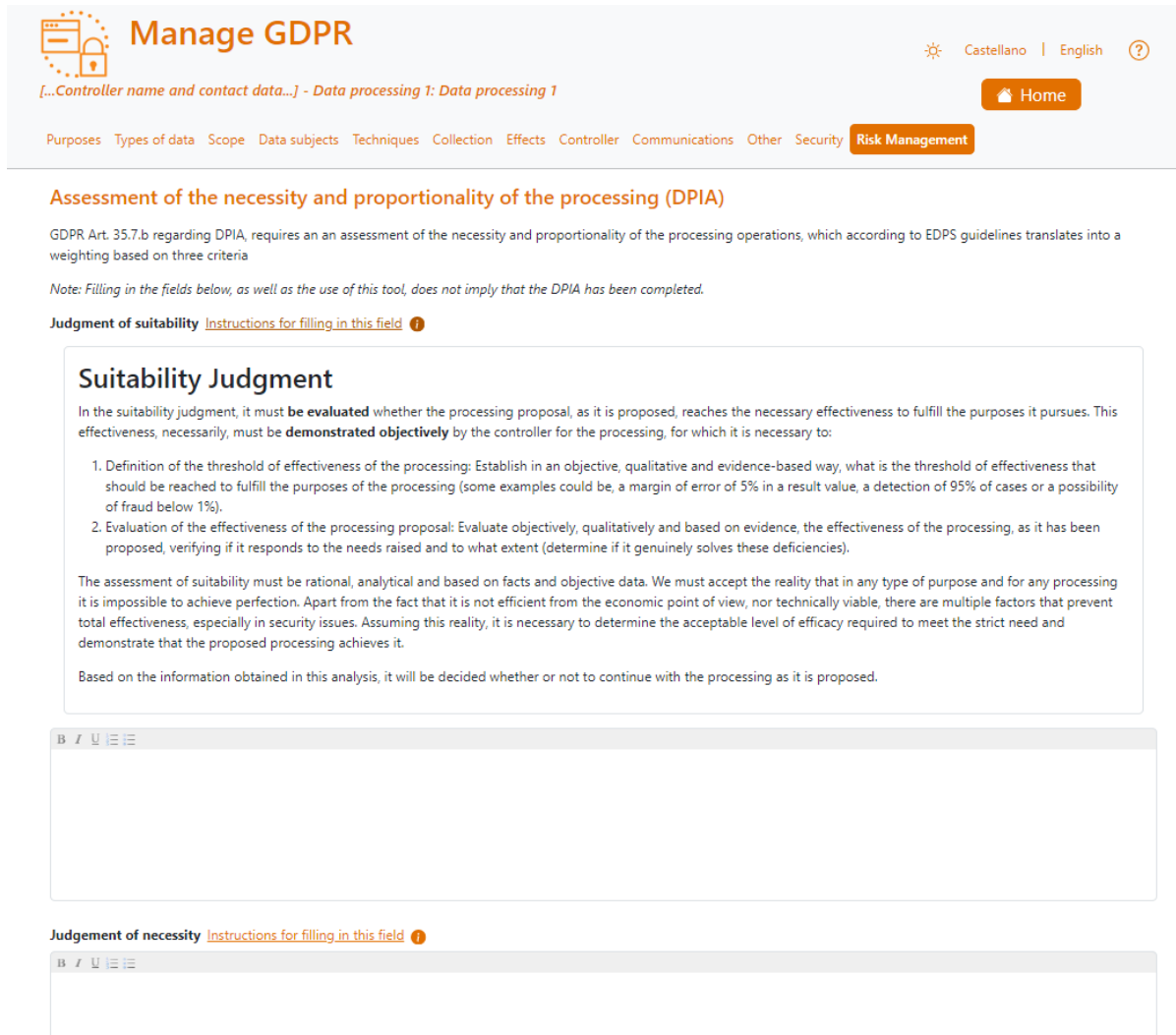
- Restricted access to data to determine solvency
- Restricted access to data that allows financial information to be deduced
- Change in the previous sense by technologies with greater reliability from the point of view of data protection, resorting for example to the use of PETs (Privacy Enhanced Technologies).
- Cancellation in the early stages of processing of certain categories of data
- Early deletion of data

Organisational mitigation measures, governance and data protection policies

- *Governance framework:* There is a specific mandate and commitment from the organisation's management regarding the management of risk to the rights and freedoms of the data subjects.
- *Governance framework:* Risk management for the rights and freedoms of data subjects is integrated into the organisation's management processes.
- *Policies embedded in procedures:* Included in the procurement procedures for products, systems or services that are to implement operations within the processing activity are the requirement for information and guarantees to ensure and be able to demonstrate that such processing complies with the GDPR.

Figure 26 Summary table

The Assessment of Necessity and Proportionality of Processing Operations (DPIA) provides help to fill in the available fields, by hovering the mouse over the underlined texts and the icon with the letter 'i' for information. However, it should be noted that the use of this tool does not automatically mean that the DPIA has been carried out.



Manage GDPR Castellano | English ?

[...Controller name and contact data...] - Data processing 1: Data processing 1 Home

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

Assessment of the necessity and proportionality of the processing (DPIA)

GDPR Art. 35.7.b regarding DPIA, requires an assessment of the necessity and proportionality of the processing operations, which according to EDPS guidelines translates into a weighting based on three criteria

Note: Filling in the fields below, as well as the use of this tool, does not imply that the DPIA has been completed.

Judgment of suitability [Instructions for filling in this field](#) i

Suitability Judgment

In the suitability judgment, it must be **evaluated** whether the processing proposal, as it is proposed, reaches the necessary effectiveness to fulfill the purposes it pursues. This effectiveness, necessarily, must be **demonstrated objectively** by the controller for the processing, for which it is necessary to:

1. Definition of the threshold of effectiveness of the processing: Establish in an objective, qualitative and evidence-based way, what is the threshold of effectiveness that should be reached to fulfill the purposes of the processing (some examples could be, a margin of error of 5% in a result value, a detection of 95% of cases or a possibility of fraud below 1%).
2. Evaluation of the effectiveness of the processing proposal: Evaluate objectively, qualitatively and based on evidence, the effectiveness of the processing, as it has been proposed, verifying if it responds to the needs raised and to what extent (determine if it genuinely solves these deficiencies).

The assessment of suitability must be rational, analytical and based on facts and objective data. We must accept the reality that in any type of purpose and for any processing it is impossible to achieve perfection. Apart from the fact that it is not efficient from the economic point of view, nor technically viable, there are multiple factors that prevent total effectiveness, especially in security issues. Assuming this reality, it is necessary to determine the acceptable level of efficacy required to meet the strict need and demonstrate that the proposed processing achieves it.

Based on the information obtained in this analysis, it will be decided whether or not to continue with the processing as it is proposed.

Judgment of necessity [Instructions for filling in this field](#) i

Figure 27 Help filling out the Suitability Trial

Once the risk assessment of a processing is completed, you must return to the Home screen (processing management) where you can generate reports and save the data processing in a file.

D. END THE SESSION, SAVE DATA, AND EXIT THE APPLICATION

Once you have finished entering or editing data processing and the corresponding risk assessment, it is necessary to save the data, because when you close the browser tab or refresh it, the data, which is in the browser's execution memory storage in the session you have opened, will be lost. The page warns you by means of a browser message.

To save the data, use the Save button on the Home page. It is important to remember that a file is saved with a predefined name, always the same: *Data_processing.aepd* (which the user can rename once saved). It will depend on the browser's configuration options whether it is saved directly to the computer's downloads folder, to a temporary folder, or by opening a file explorer to choose where.

Previously uploaded files are not modified or updated, the user will have to keep track of which is the last working file.

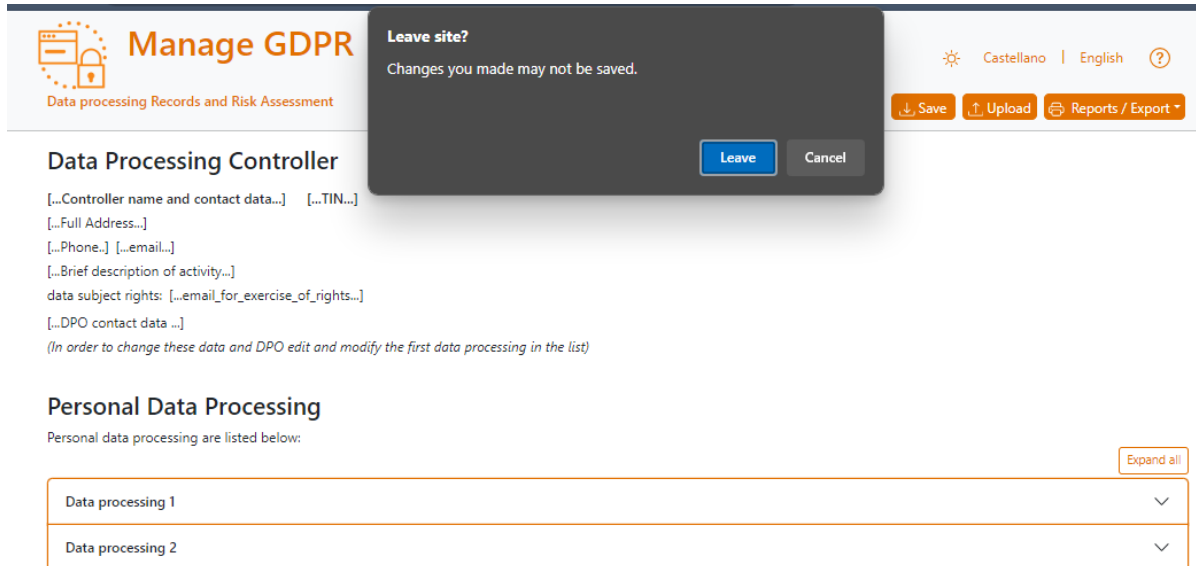


Figure 28 Warning when closing the browser tab

III. REFERENCES

- [Tool for managing the RoPA, the generation of the Inventory of Processing Operations and the risk analysis MANAGE GDPR \[jun 2023\]](#)
- [Risk management and impact assessment in the processing of personal data \[Jun 2021\]](#)
- [Website of the AEPD's Innovation and Technology Division](#)