PUBLIC REPORT ON DATA PROTECTION IMPACT ASSESSMENT

COMPASS

Marfeel Solutions S.L. (MARFEEL)

Date: March 2021

CONTENTS

CONTENTS 2
1. INTRODUCTION 3
2. SCOPE OF THE DPIA CARRIED OUT 3
3. CONTENT OF THE DPIA. 4
4. METHODOLOGY 4
5. PROJECT DESCRIPTION. 5
5.1. DPIA information 5
5.2 Project description 5
5.4 Data subjects 7
5.6 Purposes of the processing and legal basis. 8
6. NEED TO CARRY OUT THE IMPACT ASSESSMENT (DPIA) 8
7. ANALYSIS OF THE NECESSITY AND PROPORTIONALITY OF THE PROCESSING OPERATION 9
8. RISK MANAGEMENT AND CONTROL MEASURES IMPLEMENTED 9
9. CONTROLS APPLIED BY MARFEEL 10
1. Hosting of information 10
2. Confidentiality and Information Accessibility Control 10
3. Availability of information 11
4. Controls specific to the application of artificial intelligence (AI) components 11
5. Regular checks and audits 11
6. Staff 11
ii. Use of data 12
10. ACTION PLAN 13
11. CONCLUSIONS 14

1. INTRODUCTION

Within the framework of the proactive responsibility principle provided for by the General Data Protection Regulation of the European Union 679/2016, of 28 May 2016, ("**GDPR**"), and under the provisions within this regulation, the need to perform a preventive and - where appropriate - corrective analysis of the system and of the form of personal data processing is essential. The ultimate aim of this process is none other than to be able to define, identify and, if necessary, correct those aspects for correct processing while guaranteeing, in turn, the availability, integrity, security and confidentiality of the personal data processed within the framework of an activity.

The General Data Protection Regulation, Section 3, Article 35, establishes the obligation to perform a **DATA PROTECTION IMPACT ASSESSMENT** (hereinafter ***DPIA)***, as an internal process of review and control of those processing operations carried out by the Data Controller. Specifically, Art. 35.1 states:

> "*1. Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out* ***an assessment of the impact*** *of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks."*

This assessment shall aim to ensure compliance with all measures, controls and regulatory requirements necessary to safeguard the fundamental right to the protection of personal data of the natural persons that are processed.

From the perspective of the General Data Protection Regulation, A DPIA leads us to careful consideration of those technologies which are used by the Data Controller to process personal data. Increasingly, new forms of processing, the use of disruptive technologies that allow us to obtain more data and information in a short time, the use and generation of new processing and storage devices and media and their inevitable mobility make it necessary to adopt measures and controls appropriate to the risks inherent in the different forms of processing. In this regard, the correct identification of the risks associated with the forms of processing is crucial for an adequate assurance of the integrity and confidentiality of information in general, and of personal data in particular.

Undoubtedly, the adoption of security measures and proactive behaviour to guarantee and defend the rights of personal data holders means an increase and a strengthening of trust in the processing circuits, in the responsible entity and the adoption of due diligence during the processing of data referring to a human being's personal sphere. Within an increasingly globalised market with more and more diversified, relocated and virtual corporate structures, the aforementioned matters must promote the data subject's trust in the economic actors involved in this new digital economy.

2. SCOPE OF THE DPIA CARRIED OUT

This report and its contents set out, to the extent of the scope determined by MARFEEL SOLUTIONS, SL ("**MARFEEL**" or the "**Company**"), to comply with the provisions of the regulations taking into account the information provided by this report.

In this regard, MARFEEL acts as a Data Processor, so this assessment has analysed the potential processing that can be carried out using the COMPASS tool in general, the tool design,

compliance with the requirements as Data Processors and other regulations that may be applicable to MARFEEL, as well as the control measures necessary to manage the risks of loss of confidentiality, integrity and availability that are the responsibility of MARFEEL.

It should therefore be noted that Data Controllers (the "**Publishers**") wishing to use COMPASS on their websites must analyse the specific data processing operations carried out by means of COMPASS, in particular with regard to their specific characteristics, the uses they make of the software and the practical application they make of it.

3. CONTENT OF THE DPIA.

Pursuant to art. 35.7 of the GDPR, the DPIA must at least include:

a) a description of the elements involved in the processing operations planned and the purposes of the processing, including - where applicable - the legitimate interest pursued by the data controller;
b) an assessment of the necessity and proportionality of the processing operations in relation to their purpose;
c) an assessment of the risks to rights and freedoms of the data subjects *(risk analysis*)
d) the measures designed to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with the GDPR, taking into account the rights and legitimate interests of data subjects and other persons concerned.

To this end, the Publishers shall, where necessary for the type of processing carried out, seek the opinion of the data subjects or third parties involved in the processing under consideration.

In general, small changes or projects that, due to their simplicity and low privacy risks, do not entail major modifications or new uses of personal data and thus do not justify performing a DPIA are excluded from the obligation to carry out a DPIA.

4. METHODOLOGY

Firstly, this DPIA has been drawn up on the basis of the provisions laid down in the GDPR.

Likewise, the criteria of the Practical Guide for Data Protection Impact Assessments subject to the GDPR and the Data Protection Impact Assessment (DPIA) report model for the private sector, both drawn up and published by the Spanish Data Protection Agency, have been followed.

In relation to risk management, the hazards catalogue of the Margerit methodology (Book II) [1]has been taken into consideration.

Finally, with regard to risk calculation, the methodology developed and published by the French Data Protection Authority (CNIL) has been applied: METHODOLOGY FOR PRIVACY RISK MANAGEMENT[2] to estimate the magnitude of those risks that could not be avoided, obtaining the necessary information to enable the Company to take an appropriate decision on the need for preventive measures and, if necessary, on the type of measures to be taken.

---

https://administracionelectronica.gob.es/pae Home/pae Documentacion/pae Metodolog/pae Mageri t.html
[2] https://www.cnil.fr/sites/default/files/typo/document/CNIL-ManagingPrivacyRisks-Methodology.pdf

5. PROJECT DESCRIPTION.

5.1. DPIA information

DPIA Start date	**01/12/2020**
Completion Date	**17/03/2021**
DPIA controller	Metricson S.L.P.U.
The Company's Data Controllers	Juan José Nugué (Legal) Iñaki Soria (Development) Alberto Martínez (DPO)
DPIA version	1.0. - March 2021
History of changes and modifications	

This DPIA has been carried out by:

ENTITY	**MARFEEL SOLUTIONS, S.L. SL (MARFEEL)**
ADDRESS	Av Josep Tarradellas, 20 – 30, 6th Floor, 08029, Barcelona, Spain
NIF (tax ID)	B - 65651259
ACTIVITY	Platform for publishers that allows you to optimize each stage of the mobile experience to increase traffic, engagement and advertising revenue
SERVICE PROVIDED	Website marketing and analytics tool.
CONTACT	dpo@marfeel.com

5.2 Project description

The Compass tool (hereinafter referred to as "**Compass**") is a software whose main function is to measure user metrics and allow website publishers to provide users with different content or offers, based on their browsing profile. This is done through information collected by cookies or other similar tracking devices configured on the website.

Compass uses artificial intelligence (AI) components - namely algorithms - which operate through software and allow personal information to be collected and reasoning to be applied in order to reach conclusions.

In this regard, Compass receives information about each user (their browsing profile) and scores it. The segmentation proposed by Marfeel for this scoring (and the one used by default in the software) is as follows:

a) On the one hand, the segmentation known as RFV (Recency, Frequency and Value), one of the most widely used in the field of marketing:
   - The "Recency" indicator analyses when the user last interacted with the website within the time range determined for each case, depending on the publisher.
   - Through the "Frequency" indicator, the number of times the user has interacted with the website is analysed.
   - Through the "Value" indicator, the user's loyalty to the website is calculated.

b) Segmentation is carried out based on the content visited ("Content Scoring").

Notwithstanding the above, some parameters must be defined or validated by the Publisher - who will be the Data Controller - in order to complete this segmentation, such as which actions count in the sum of the indicators or the time frame in which this segmentation will operate.

Finally, the objectives or actions to be implemented with each group of users resulting from the application of the previous segmentation are established. Compass makes it possible to automate actions once the different user groups have been established. For example, on a website offering digital press content, users with a high loyalty level can be automatically offered paid subscription options and/or, in the case of Content Scoring, content cam be suggested that is similar to what the user usually consumes.

Notwithstanding the above, the Website Publisher may establish other types of segmentation in the tool, based on their own criteria.

5.3. Most significant processing operations carried out by MARFEEL

PHASE	OPERATIONS
INPUT	Acceptance of the use of cookies on the user's device and collection of their browsing information.
CLASSIFICATION / STORAGE USE/PROCESSING	Storage of information on virtual servers of the hosting provider, managed by MARFEEL. To collect metrics User scoring, according to metrics Implementation of automatic decision-making according to scoring, based on instructions from the Publisher. Preparation of statistical reports on the use of the website. Sending users suggestions, offers for subscription or to purchase products and services.
DISCLOSURE	Marfeel makes no disclosures (except for legal transfers)
DESTRUCTION	Deletion of personally identifiable information within the time limits indicated by the Publisher (the - aggregated - statistical information obtained from the data processing is kept indefinitely).

5.4 Data subjects

Users who access the publisher's website (and, if applicable, who agree to the use of COMPASS)

5.5.- Personal data collected by COMPASS in the default configuration

CLASS A. PERSONALLY IDENTIFIABLE DATA

Description

No personally identifiable data is collected

CLASS B. Other personal data

Description

User ID (only Publisher request)

CLASS C. Calculated /inferred data

Description

Media engagement (RFV segmentation) Favourite sections (or another label as defined by the Publisher) Propensity to subscribe/register/purchase Churn risk (stopping using services).

CLASS D. Personal data collected (the data have been obtained by devices or applications which, autonomously, without any specific action on the data subject's part, collect various information - cookie information, browser used, mobile device information, geo-positioning coordinates, IP address, connection time, etc.).

Description

Unique browser identifier

IP anonymising last byte

Website browsing (e.g., URL, title, section, etc.) Operating system and version

Browser and version

Scroll

Duration of the visit

Actions performed by the user (depends on customer labelling - for example: User subscribes, user registers, user agrees to push notifications.)

5.6 Purposes of the processing and legal basis.

Purposes	Data used	Legitimation
To collect metrics	Class B, Class C, Class D	The legitimate basis will be those decided by the Publisher, although, based on the applicable regulations, it should be the consent given by the user when he/she accepts the cookies on the website.
User scoring (user segmentation), according to metrics.	Class B, Class C, Class D	The legitimate basis will be those decided by the Publisher, although, based on the applicable regulations, it should be the consent given by the user when he/she accepts the cookies on the website.
Implementation of automatic decision-making according to scorings, based on instructions from the Data Controller.	Class B, Class C, Class D	The legitimate basis will be those decided by the Publisher, although, based on the applicable regulations, it should be the consent given by the user when he/she accepts the cookies on the website.

6. NEED TO CARRY OUT THE IMPACT ASSESSMENT (DPIA)

The GDPR provides for only a few cases in which it is mandatory to carry out the DPIA. Firstly, it shall be necessary "*Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons* [...]" (art.35.1, GDPR). In addition, three particular cases are established where it will always be mandatory to carry out this type of assessment:

1. a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person;
2. processing on a large scale of special categories of data referred to in Article 9.1, or of personal data relating to criminal convictions and offences referred to in Article 10; or
3. a systematic monitoring of a publicly accessible area on a large scale.

The use of the expression "in particular" in the introduction to Article 35.3 GDPR refers to the fact that this list is not exhaustive, which means that the existence or non-existence of "high risk" should always be taken into account, and therefore a processing activity should always be analysed beyond the three examples indicated in this Article.

The characteristics of the data processing have been analysed in relation to the indicative criteria of "high risk" that determine that the DPIA has to be carried out, based on the

assumptions of art. 35.2 GDPR, the lists of mandatory or excluded assumptions drawn up by the Spanish Data Protection Agency, the guidelines of the former Article 29 Working Group and the cases of "higher risk" included in Organic Law 3/2018, of 5 December, on the Protection of Personal Data and the guarantee of digital rights.

From the analysis carried out, it can be concluded that the data processing carried out using MARFEEL's COMPASS tool in its basic configuration would meet several of the criteria for "high risk" from the outset.

It must therefore be concluded that data processing **MUST BE SUBJECT TO AN IMPACT ASSESSMENT** in order to analyse the risks to which they are exposed and their impact on data subjects in detail.

7. ANALYSIS OF THE NECESSITY AND PROPORTIONALITY OF THE PROCESSING OPERATION

The necessity and proportionality analysis carried out for the purposes of this analysis has been performed partially, on the basis of the COMPASS operation, without taking into account any special characteristics that each individual Publisher may have or any additional data processing beyond that provided for by the tool by default.

In general, the tool is based on the RFV and Content Scoring parameters, unless the Publisher includes a change in this regard. The choice of RFV as an engagement indicator was made on the basis of its effectiveness in the context of advertising and marketing.

The processing of personal data is required to fulfil the purposes of Compass, as these purposes require the initial collection of personal data (even if it is later anonymised when individualisation is no longer necessary), and further processing (content, subscription or purchase offers suggestions) is targeted at individual, specific users, which is not possible without the processing of personal data.

The use of artificial intelligence techniques is necessary to carry out the processing performed by Compass, given the tool's goal, which is the personalisation of content or advertising actions based on the type of user. In these processes, Artificial Intelligence allows this segmentation to be carried out efficiently, and there are currently no equivalent measures, technical or otherwise, that allow content or offers to be suggested to users on a website in such an effective and rapid manner without the data processing carried out by Compass.

The implementation of Compass also has a clear user benefit, as the user will be treated according to their interest in the media and the company whose website they are visiting, instead of receiving generic suggestions that may or may not include content relevant to them.

8. RISK MANAGEMENT AND CONTROL MEASURES IMPLEMENTED

Risk management is the process of identifying, analysing and assessing the likelihood and impact of the possibility of a risk materialising in order to establish preventive, corrective and mitigating actions to minimise the level of risk exposure.

In the first phase of the DPIA, a sufficient level of information has been described to be able to identify the threats and risks to which the processing of personal data is exposed in relation to the privacy of individuals.

In addition to the description, Article 35.7 of the GDPR states that DPIAs contain an assessment of the risks to the rights and freedoms of data subjects and the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with the GDPR, taking into account the rights and legitimate interests of data subjects and other affected persons.

Therefore, in order to identify and assess the risks, the following steps have been taken:

- Identifying the source of the risks, i.e., analysing the potential scenarios in which personal data may be exposed to risk.
- Analysing the situations that generate risk, taking into account the factors and characteristics that may come into play in determining the level of risk involved.
- Assessing risks, taking into account the likelihood of an undesired event occurring and the impact it may have (consequences).

The controls implemented to ensure compliance with legal requirements pursuant to the GDPR have also been assessed, which has made it possible to determine the status of regulatory compliance.

Likewise, the security measures implemented or planned for the processing operation analysed have been assessed.

9. CONTROLS APPLIED BY MARFEEL

Some of the controls applied by Marfeel to manage the risks for which it is responsible are listed below:

1. Hosting of information

We use the services of a hosting service provider: SCALEWAY SAS, whose virtual servers are located, according to their website, in the European Union, specifically: Paris (France), Amsterdam (Netherlands) and Warsaw (Poland).

The supplier, according to its own information, has the following security certifications: TIER 3, Healthcare HDS, ISO 27001, ISO 50001 and it applies security measures such as access control and continuous surveillance.

More information on SCALEWAY's Information Systems Security Policy can be found at the following link: https://www.scaleway.com/en/pdf/PSSI_en.pdf.

2. Confidentiality and Information Accessibility Control

MARFEEL has a security policy which is applicable to all employees and subcontractors. All employees, as well as subcontractors, sign confidentiality agreements, committing themselves to the secrecy of all information and data to which they have access by virtue of their duties.

An access control policy has been established and defined, with identity management, implementing access roles and privileges in all MARFEEL systems based on the "need-to-know" principle, according to the user's profile.

Each of the users who access the systems is properly identified and authenticated. A password policy has been implemented for user and administrator accounts, which includes complexity rules, depending on the level of access.

However, the Publisher shall be solely responsible for the confidentiality and security of their Compass control panel access credentials.

A trusted environment has been established by implementing perimeter measures for network partitioning and confinement, to prevent unauthorised access to systems and data, and to prevent and combat malware.

HTTPS security protocol is applied, which allows a secure connection to be established between the server and the website.

3. Availability of information

Marfeel performs redundant backups of data, applications, operating systems and of the internal system. In this regard, only system administrators can access backups, for justified reasons, such as data recovery in case of data loss.

The frequency of backups depends on the type, sensitivity and volume of data. In addition, regular data recovery tests are carried out to ensure that the backups are working properly.

Furthermore, disk and RAM usage monitoring measures are applied to detect, prevent and combat possible system crashes due to resource exhaustion or denial of service attacks.

4. Controls specific to the application of artificial intelligence (AI) components

RFV algorithms are tested and deterministic, i.e., the result of the application of the algorithm has been tested on large data sets to verify that the result obtained is always the desired one.

The segmentation suggested for this scoring (default and design scoring) is the result of direct relationships. Compass does not use variables of interest that are not directly measurable.

In addition, data monitoring mechanisms have been implemented to assess the component's behaviour during its interaction with the environment.

In this regard, checks are established and scheduled in order to review the functioning of the algorithm and the whole process of data collection and analysis.

5. Regular checks and audits

At Marfeel, pentesting (or penetration tests) of Compass and the rest of the information systems is periodically performed by specialised personnel so as to detect vulnerabilities and determine the application of additional security measures at a technical level.

All Publishers have a support channel to notify Marfeel of any incident or anomalous behaviour detected in Compass.

6. Staff

Marfeel staff in charge of making decisions regarding security measures are sufficiently trained and qualified.

7. Privacy principles

i. Data minimisation and retention period

Personal information that identifies the user (or may lead to the user being identified indirectly) and that information relating to the individual profile is expected to be retained only temporarily, for a period of time indicated by the Publisher based on the purposes of the processing, although, by default, it is recommended that a period of 30 days be set. Subsequently, only anonymised information shall be kept, for statistical purposes, in order to be able to assess the evolution of the use of the website in question.

The data collected are a result of the proven and deterministic RFV algorithms.

The minimum data necessary to be able to obtain statistics and suggest content to users based on RFV and Content Scoring parameters is kept as well. By default, all of the above information relating to data subjects undergoes pseudonymisation, meaning that each data subject will be assigned a randomly generated identification code in order to separate the data from individually identifiable information (e.g., IP or MAC address), thus ensuring that no data that could reveal the identity of a data subject are stored.

ii. Use of data

Marfeel does not use the data contained in Compass except for the uses expressly authorised in the service contractual agreement, which contains an agreement by the data processor to undertake data-processing. Marfeel undertakes to use personal data in accordance with the customer's documented instruction. Furthermore, Marfeel does not sell or transfer data to third parties, except to government agencies, exclusively in the event that there is a legal obligation to do so.

iii. Transparency

Marfeel has created a specific Privacy Policy for the Compass tool in order to ensure that users can access detailed information about the processing carried out through Compass (in its default settings).

This information is made available to Publishers to post on their websites as an addition to their own information.

However, it is ultimately the Publisher who must comply with the duty of information and explain to the user the ultimate purposes of the processing of their data through the tool and any other purposes that may be carried out as a result of its use.

iv. Rights of data subjects

As set out in the data processor's service agreement, in the event that the data subject contacts Marfeel directly to exercise their rights, an e-mail and postal address has been included in Compass' specific Privacy Policy for data subjects to send their requests free of charge.

Marfeel has made a contractual commitment to the Publisher to send it any rights requests it receives directly and, in the event that the Publisher includes as an instruction the resolution of the requests by Marfeel, they have a protocol that includes information on how to proceed with the data subject, depending on the request made.

v. Data Protection Officer

Marfeel has appointed a Data Protection Officer to supervise compliance with data protection regulations in all of Marfeel's processes and areas of activity, and has given notice thereof to the Spanish Data Protection Agency.

vi. International transfers

We may transfer your personal data to Marfeel's subsidiary: Marfeel Colombia S.A.S., located in Colombia, a country outside the EEA (European Economic Area) for technical support purposes. In this respect, the relevant standard contractual clauses approved by the European Commission have been signed, ensuring that European data protection standards are applied.

The servers hosting the database are located in the European Union.

vii. Security breaches

Any security incident detected is handled according to a formalised and validated procedure, which is known to all employees and system users. This procedure contains guidelines for the detection, analysis, internal communication and notification of security breaches to the competent authorities, as well as to customers who may be affected by the incident, where such communications are necessary.

10. ACTION PLAN

As a final step in conducting a DPIA, an action plan has been drawn up describing all the initiatives to be undertaken to implement controls and help reduce the risk of the processing operation which is under assessment to a level considered acceptable. The action plan includes:

- Description of the set of mitigating measures and additional controls that the entity plans to implement so as to lower risk levels.
- Person in charge of the implementation.
- Timeframe for implementation.In this respect, a maximum time limit has been established within which the control measures included in the action plan must be implemented. If the time limit is exceeded, the controller should demand that the processing be stopped until the appropriate measures are put in place.

Of course, the DPIA will need to be revised, both before the Publisher (the Controller) implements this tool, and in the event of modification of the data processing or the incorporation of new functionalities. The DPIA will need to have a broader or smaller scope depending on the depth and magnitude of any changes made.

Thus, the classical Deming Wheel or Cycle (plan–do–check–act or plan–do–check–adjust) should also be observed in implementing and developing the DPIA.

11. CONCLUSIONS

The result of this DPIA of the data processing carried out through COMPASS, in its default configuration and without taking into account special characteristics of the data controller or data processing other than those provided for, is favourable, provided that the established Action Plan is complied with, the proposed control measures are implemented and no processing not provided for in this DPIA is carried out by the Data Controller.