MARFEEL WHITEBOOK OF BEST PRACTICES

This Document governs the roles and responsibilities related to the Processing of Personal Data and related security procedures to the extent applicable to the Services provided by MARFEEL SOLUTIONS SL.

Marfeel Solutions, S.L.

CONTENTS

Content

INTRODUCTION

In order to ensure that natural persons are not deprived of the protection to which they are entitled, and to adapt the regulatory framework to technological reality and to large-scale data processing, Regulation (EU) 2016 / 679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 (GDPR) it is a necessity to adapt the processes and flows of information processing to the new normative scenario.

This Document governs the roles and responsibilities related to the Processing of Personal Data and related security procedures to the extent applicable to the Services provided by MARFEEL SOLUTIONS SL.

SCOPE

This document is public and it is directly addressed to MARFEEL employees and DPOs from publishers and service providers.

The obligations described in the present Document will be brought to the attention of all MARFEEL employees, in order to comply with the obligations derived from the data protection applicable regulations, especially the GDPR.

COMPANY IDENTIFICATION

Name	MARFEEL SOLUTIONS, S.L.
VAT Number	B65651259
Address	Av Josep Tarradellas, 20-30 P.6 08029 - Barcelona (Spain)
Activity	Related Information Society Services and computer technologies. Web optimization and advertising placement.
Offices	Spain, US
Security	Alberto Martínez Laguía-Joan Tomás i Buliart
DPO	dpo@marfeel.com

1 – CULTURE OF SECURITY

1.1.- Selection Criteria

In the process of selecting and hiring staff, MARFEEL is very aware of the need for confidentiality. So much so, that as well as their employment contract, each staff member is asked to sign an annex to the contract which, among other things, deals with CONFIDENTIALITY and NON-DISCLOSURE. This is an extract:

"Both during the term of your Contract of Employment with the Company and after its termination, you must observe the strictest secrecy in relation to the nature and characteristics of the business and affairs of the Company in respect of all confidential information, that is to say, anything that is not generally known outside the Company, whatever the subject matter may be. The obligation to maintain professional secrecy requires you not to make any use of any information concerning any business or potential business of the Company or its customers nor to disclose to anybody without prior consent any information or trade secret or confidential information regarding the Company's business or that of its customers, nor to provide any information concerning any inventions, campaigns, transactions, research, business plans or market research, made or undertaken by or on behalf of the company or its customers."

Even so, MARFEEL is going further in relation to data security by putting in place a culture of security in the company, in addition to its confidentiality and non-disclosure agreements. The deployment of this culture involves: educating our people about cybersecurity in the context of the internal security policies, rules and procedures of the business; monitoring by the Security Committee of implementation of established good security practices; and continuously undertaking security=related awareness-raising activities with staff. In parallel, we are also taking steps in Human Resources to ensure that new employees at MARFEEL adapt to the corporate culture.

1.2.- Staff training at MARFEEL

At MARFEEL we recently held structured staff training. This is the course content:

- What is GDPR? Definition, scope and differences with the current policy
- Financial and legal risks for the company
- Updates on MARFEEL General Terms of Services (GTOS):
    - Definition of MARFEEL as a Data Processor
    - Solutions provided by MARFEEL to obtain consent from users who visit MARFEEL client's websites
- Consent Management Platform (CMP) and consent flow
- Global Vendor List
- IAB standard framework and MARFEEL's own CMP

After the course, attendees were tested. The test took the form of 20 questions related to the training. These were the results:

- Employees tested: 31
- Average score: 82.6% (16.5/20)
- Average time taken for test: 00:09:21

The action plan for those members of staff who scored less than 75% was to repeat the course and the test.

The course was also provided to MARFEEL's customers in a Webinar on 23/05/2018. The statistics are as follows:

- Length: 53 minutes
- Customers registered: 61
- Attendance: 20
- Questions answered: 27

The Webinar is available at:
https://atenea.marfeel.com/atn/marfeel-press/systems-requirements/gdpr-general-data-protection-regulation/gdpr-webinar#

1.3.- Security Plan

MARFEEL has a Security Plan which is periodically updated and which is available to members of the public who request it via dpo@marfeel.com.

2 – SECURITY BODIES

2.1.- Security Committee

MARFEEL has a Security Committee which meets periodically and has been involved in decisions relating to security at the company. The Committee has external advisers (technical and legal) who have advised MARFEEL in relation to GDPR.

Membership of Security Committee

Made up of 9 people, of whom 7 are from MARFEEL's Technical Department:

Technical Department	Finance Department	Marketing Department
CEO Engineering Director 2 Product Managers Design Manager 2 Team Leaders	Financial Controller	Marketing VP

Apart from the Security Committee, there are 5 people who have managed the process since the beginning and who have been directly involved in the daily tasks needed to bring MARFEEL into line with the new requirements of the General Data Protection Regulation and monitoring of compliance. They are: CFO, Financial Controller, Systems Manager and the 2 Product Managers.

The Committee has a dedicated communication channel at gdpr@marfeel.com. This channel is used for discussion of security practices and procedures which might be introduced in the Business to support the DPOs and any queries that might arise with regard to data protection.

2.2.- Security Officers

Apart from the Security Committee and the 5-member operational core team just described, MARFEEL has a Security Officer who is attached to the legal/financial team and the overall management of the project (Alberto Martínez, Financial Manager), and an officer who is responsible for technical implementation (Joan Tomàs i Bulliart - Systems Manager).

Although both attend meetings of the Security Committee, they are independent from it since they are not involved in the processing of any personal data.

Both have received relevant training from legal and technical advisers and their focus is internal supervision and continuous compliance with GDPR.

Name of Officer:	Alberto Martínez Laguía
Area or Department:	Finance
Contact email address:	dpo@marfeel.com
Date of appointment:	13 April 2018
Term of appointment:	Indefinite

Particular functions of Security Officer:

1. To monitor compliance with all requirements of GDPR and Spanish law in the same or related areas.

2. To prepare and keep up-to-date the rules for the use of information systems.

3. To keep up-to-date the manual in respect of automated and non-automated processing.

4. To monitor compliance with the security requirements set out in the manual.

5. To assemble and describe the security-related measures, norms, procedures, rules and standards adopted by MARFEEL.

Delegation of Authority.

The Security Officer may delegate such of his or her functions as he or she sees fit according to the complexity of processing, particularly in those cases where technical monitoring of processing or systems is required.

Designated Deputies:

Name of Deputy:	Joan Tomàs i Buliart
Area or Department:	Systems
Contact email address:	dpo@marfeel.com
Date of appointment:	13 April 2018
Term of delegation:	Indefinite

3 – SECURITY MEASURES

3.1.- Membership of IAB Europe (Interactive Advertising Bureau)

MARFEEL is a member of IAB Europe. IAB Europe, as it says in its mission statement, is "*The leading European-wide industry association for digital advertising ecosystems. Its mission is to promote the development of this innovative sector and ensure its sustainability by shaping the regulatory environment, demonstrating the value digital advertising brings to Europe's economy, to consumers and to the market, and developing and facilitating the updating of harmonised business practices that take account of user expectations and enable digital brand advertising to scale in Europe."*

IAB Europe has played the leading role in communication and training of industry participants in relation to data protection and continues to promote the development of online publicity through practices such as supporting its members in relation to regulation, establishing business standards, offering education and training in the area, etc.

MARFEEL is not only a member of IAB Europe but has also registered its own CMP (Consent Management Platform) and made it available to other members. Further, all the Adnetworks that MARFEEL works with are members of IAB, which means that they have included the relevant standards in their routine practices.

https://iabspain.es/asociados/quien-es-quien/

4 – DATA ANONYMISATION

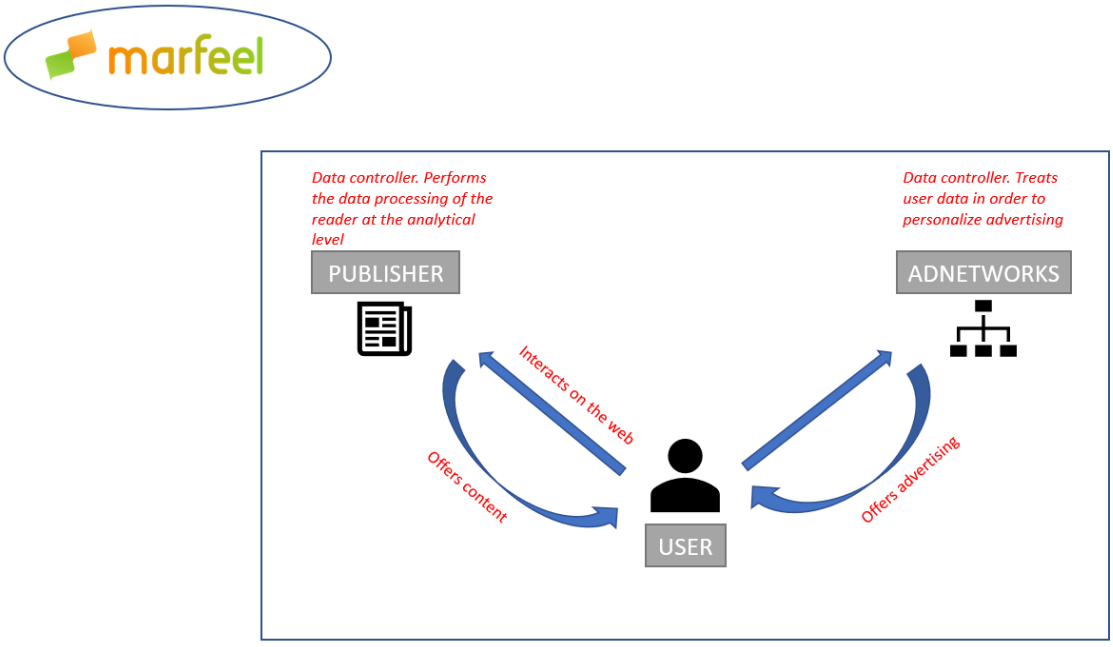
MARFEEL does not act as a Data Processor as it does not hold any personal data for users. Even so, it is the Data Processor for Publisher data: banking information, workers, etc., but it does not process or control any user information, which is fully anonymised.

The company is an intermediary between publishers (MARFEEL's customers), for whom MARFEEL optimises the website and manages advertising, and the Adnetworks. MARFEEL cannot have access to any personal information that would allow the identification of any individuals through the provision of services to its customers.

In fact, MARFEEL links user visits to the websites of publishers to an alphanumeric code which is anonymous and non-reversible, in the sense that the code cannot be used to identify an individual. The code is what is shared with the Adnetworks to enable them to display their advertisements.

Next, we will show the information flows between the different agents operating in the industry and how user information is processed:

FLOW DIAGRAM OF PERSONAL DATA PROCESSING



5 – INFORMATION PROCESSING

5.1.- Classification of information

For purposes of this Manual, information managed by MARFEEL can be put in one of three categories:

1. **Public**: Information that has been disseminated or provided to third parties through any communication medium or any physical medium.

2. **Restricted:** Information intended to be used exclusively by MARFEEL employees in the performance of the routine tasks of the business.

3. **Confidential:** Information which, if it were to be disclosed, could reveal trade secrets or constitute a breach of the Law on Protection of Personal Data or any other law which requires the use of data security measures, reduce MARFEEL's competitive advantage or cause material harm to the business or reputation in the marketplace of MARFEEL.

5.2 Register of data processing

PROCESSING	INT. TRANSFER DATA	DESCRIPTION
HUMAN RESOURCES	Yes	Details of MARFEEL employees such as: Address, email address, National Insurance Number, etc.
SUPPLIERS	Yes	Business details of suppliers
CVs	Yes	CVs of candidates to join MARFEEL. Short term electronic storage
MARFEEL.COM USERS	Yes	Users who visit www.marfeel.com (not users of the websites of the customers of MARFEEL -Publishers-)
PUBLISHERS	Yes	Business details of Publishers
EMAIL UPDATES/NEWSLETTERS	Yes	Newsletter sent to MARFEEL customers who have given their consent
BUSINESS CONTACTS	Yes	Data stored on a short-term basis for potential customers related to professional or business contacts. In the case of contacts with individuals protected by the GDPR, their consent has been obtained and/or they have been informed of the processing of their data
FINGERPRINT ACCESS	Yes	MARFEEL employees gain access to the offices by fingerprint entry. The system does not store any biometric information and uses a code which allows it to re-generate the fingerprint.
WHISTLEBLOWERS	Yes	A communication channel which allows staff to send their demands or complaints about MARFEEL

5.3 Media used in information processing

The aim of MARFEEL in relation to media used in information processing is the paperless office for security, space and environmental reasons. This means that to the greatest possible extent all the businesses and business units within MARFEEL use information storage software or a computerised document management system which progressively displaces paper, scanning documents to retain them digitally (as with invoicing, contracts or Board Resolutions).

Similarly, it should be noted that publishers, along with the content of their websites, are stored in TIER 1 hosting providers and never at MARFEEL's offices (the business does not have any servers at its offices). Below, we list the hosting providers and the locations of their servers

HOSTING SERVICES				
Provider	**Certified**	**Stores users' personal data?**	**Service**	**CPD location(s)**
Amazon Web Services	Yes	No	Hosting service (servers)	Ireland
Hetzner	Yes	No	Hosting service (servers)	Germany
Kimsufi	Yes	No	Hosting service (servers)	France

All MARFEEL servers are in countries belonging to the European Union, and as such within the scope of the GDPR.

OTHER SERVICES (NOT HOSTING)				
Provider	**Certified**	**Stores users' personal data?**	**Service**	**CPD location(s)**
Google cloud	Yes	No	Gateway	For the whole world
Fastly	Yes	No	CDN (Content Delivery Network)/Cache storage service	USA, Brazil, Belgium

Finally, paper documents are stored in locked cabinets which can only be accessed by authorised personnel. This information and the authorised personnel are:

Document	**Under lock and key**	**Authorised personnel**
Invoices	Yes	Finance Department
Written documents	Yes	Finance Department
Employment contracts, indemnities and P45s	Yes	Human Resources Department

6 – INCIDENT MANAGEMENT

6.1 Reporting of incidents to the Controlling Authority

In the event there is a personal data security breach, the data controller will notify the competent controlling authority without undue delay and, if possible, no later than 72 hours after it has been detected, unless it is unlikely that such a breach of security constitutes a risk to the rights and freedoms of natural persons.

If the notification to the supervisory authority does not take place within 72 hours, it must be accompanied by an explanation for the delay.

As a minimum, the notification must:

a. detail the nature of the personal data security breach, including, when possible, the categories and the approximate number of data subjects affected, and the categories and approximate number of personal data records affected;
b. communicate the name and contact details of the data protection officer or other contact point where more information may be obtained;
c. detail the possible consequences of the personal data security breach;
d. detail the measures adopted or proposed by the data controller to remedy the personal data security breach, including, if applicable, measures adopted to mitigate possible negative effects.

If it is not possible to provide the information simultaneously, and to the extent that it is not, the information will be provided gradually without undue delay.

The data controller will document any personal data security breach, including the related facts, its effects and the corrective measures adopted. This documentation will allow the controlling authority to verify compliance with the provisions of this article.

6.2 Notification of incidents to the data subject

When the personal data security breach is likely to entail a high risk to the rights and freedoms of natural persons, the controller will inform the data subject without undue delay.

The information given to the data subject will detail in clear and simple language the nature of the personal data security breach and will contain the following information, as a minimum:

As a minimum, the notification must:

a. communicate the name and contact details of the data protection officer or other contact point where more information may be obtained;
b. detail the possible consequences of the personal data security breach;
c. detail the measures adopted or proposed by the data controller to remedy the personal data security breach, including, if applicable, measures adopted to mitigate possible negative effects.

However, as previously stated, the communication to the data subject will not be necessary if one of the following conditions is met:

a. the controller has taken the appropriate technical and organisational protection measures and these measures have been applied to personal data affected by the personal data security breach, in particular those that make the personal data unintelligible to anyone who is not authorised to access them, such as encryption;
b. the controller has taken further measures to ensure that there is no longer a likelihood that the high risk to the rights and freedoms of the person concerned will materialise;
c. a disproportionate effort would be entailed. In this event, a public announcement or a similar measure through which the data subjects are effectively and equally informed will be chosen instead.

If the data controller responsible has not yet informed the data subject of the personal data security breach, the supervisory authority, after considering that the probability that such breach entails a high risk, may require the data controller to do so or may decide that one of the conditions mentioned is fulfilled in order not to issue the above notifications.

7 – LOGICAL ACCESS CONTROL

- Each profile has associated privileges, according to the post and duties of the user who requests access.

- Control of access to files containing personal data will be at the following levels:

    - Control of access to processing
    - Control of access to protected fields
    - Control of access to protected records
    - Control of access to groups of records

- According to the user's privileges, the user will only be able to access those data and resources required for the performance of his or her functions.

- Each user's privileges will also determine the type of tasks that they can carry out, as per the following levels:

    - Creation of new fields
    - Deletion of fields
    - Adding new records
    - Deletion of records

8 – MEDIA MANAGEMENT

8.1.- Back-up copy protocol

The creation of copies or reproduction of documents containing personal information may only be carried out under the supervision of the security officer.

The destruction of unneeded copies or reproductions must be carried out in such a way as to preclude access to or recovery of the information contained in them.

8.2.- Document transfer protocol

Whenever documents containing personal data are physically moved from place to place, it is essential to adopt measures which prevent access to or manipulation of the information being transferred.

8.3.- Custody and retention protocol

While documents containing personal data have not been stored in the document storage facilities, whether because they are being revised or processed and whether before or after initial archiving, the person who has custody of any such document must look after it and prevent access by unauthorised third parties at any time.

Cupboards, filing cabinets or any other furniture in which non-computerised files containing personal data may be stored are situated in areas to which access is controlled under lock and key or similar means. These areas are closed at all times when it not necessary to access documents subject to processing.

8.4 Destruction and re-use of media protocol

Magnetic media intended for disposal or re-use must first be degaussed in order to ensure total deletion of all data.

Alternatively, other systems which ensure that data cannot be recovered by any means, even through the use of specialised forensics programs, may be used.

In the case of paper documents, destruction will be carried out in such a way that the output of the process prevents access to the data that a document contained. To that end, either shredders that meet that requirement or the services of a confidential document destruction company may be used, and any such provider will be required to certify destruction and allow audit of destruction.

9 – BACK-UP COPIES OF INFORMATION STORED ON THE SERVERS

MARFEEL has a data back-up and recovery procedure which ensures the restoration of data to the condition at the time of its loss or destruction.

The procedure consists in making weekly back-up copies of all information which is carried out on an external server of the American multi-national Amazon Web Services. The servers holding the copies are in Europe.

We also use servers belonging to Hetzner and Fastly, and Google cloud, whose servers are in the USA but which have been certified under the Privacy Shield between the EU and the USA.

Should there be an incident which leads to the destruction of information, MARFEEL will implement its procedure for reporting, processing and recording incidents set out in this manual and will recover the information that has been destroyed. Should recovery prove impossible, MARFEEL will request the most recent back-up copy and restore the information destroyed.

Every six months, the security officer will check that the procedures for producing back-up copies and for data recovery have been correctly defined and applied and work as required.

Servers contracted to external providers (AMAZON WEB SERVICES, HETZNER) carry out recovery.

MARFEEL also makes back-up copies of the information on Alice and Insight (these copies are on Hetzner's servers).

MARFEEL does not make copies of Publishers' content given that in the event of loss such content is easily recoverable.

Time taken to restore lost information: several hours.

-SLA Amazon Web Services: which guarantees a 99.99% recovery of lost information.

-SLA Google Drive: (https://cloud.google.com/storage/SLA) which guarantees a 99.99% recovery of lost information.

In the case of high level data, the back-up copy and the recovery procedures must be kept in a different place from the location of the computer systems on which processing is being carried out in accordance at all times with the security measures required by the Law on Protection of Personal Data.

10 – DATA PROCESSORS

SERVICE PROVIDER	SERVICE PROVIDED	LINK GDPR COMPLIANCE
GOOGLE LTD.	Cloud data storage	https://cloud.google.com/security/gdpr/
AMAZON	Cloud data storage	https://aws.amazon.com/es/compliance/gdpr-center/
HETZNER	Cloud data storage	https://www.hetzner.com/rechtliches/datenschutz/?country=es
FASTLY	Cloud data storage	https://www.fastly.com/data-processing
MICROSOFT	Cloud data storage	https://www.microsoft.com/en-us/trustcenter/privacy/gdpr
MARFEEL US LLC	Creation of customer network in the USA	Marfeel Solutions S.L. subsidiary
SALESFORCE.COM INC	CRM	https://www.salesforce.com/eu/campaign/gdpr/
ACTON	Telecommunications services	https://www.privacyshield.gov/participant?id=a2zt0000000TOMVAA4&status=Active