GDPR COMPLIANCE GUARANTEE

GDPR Compliance guarantee

As of today, Mobile Leaves Corp is deeply committed to complying with the regulations for the protection of personal data of the country of origin of our users and their respective users.

This also applies to compliance with data protection regulations applicable to the EU, where it governs the GDRP (European Regulation of Protection of Personal Data 679/2018).

What kind of actions does Mobile Leaves Corp carry out to guarantee the rights of the interested parties from the EU?

1. Application by default in all our processes of the principles and requirements of the GDPR regulation:

This regulation is one of the most complete and guarantees currently in force, therefore, apply its principles imply not only being aligned with European legislation, but also being one point above regarding compliance with the regulations of third countries.

Principle of limiting treatment to the bare minimum: By Mobile Leaves Corp only the necessary data is requested to be able to carry out the contracting of the service and its correct management. This implies that the categories of data that it deals directly refer only to data identification of the client who wants to contract our QR code services.

Application of security measures appropriate to the type of treatment: Mobile Leaves Corp has contracted the data storage service with the company Amazon Web Services, a company widely accredited and that has the most information security certifications demanding of the market. You can have detailed information about the certifications regarding information security at this link: https://aws.amazon.com/es/compliance/programs/

This implies that the data that can be generated and stored through the QR codes that are active will be stored safely. The Amazon Web Services S3 module has encryption mechanisms for information in transit and at rest, as well as the possibility of establishing and restricting access and monitoring them. You can get more information at https://docs.aws.amazon.com/es_es/AmazonS3/latest/dev/DataDurability.html

2. Establishment of Standard Contractual Clauses

While the EU and the USA define a protocol that updates the adequate mechanisms of international transfer of personal data between both territories, and until November pronounced by the corresponding control authorities, the adaptation to regulations remains in force of the Standard Contractual Clauses. They define the obligations of the data importer (Mobile Leaves Corp) and the security measures applied, together with the definition of the data that is collected, stakeholder categories, etc.

You can have a copy of our CCT HERE

3. Categories of data affected

Mobile Leaves Corp only asks its customers for identifying information in order to carry out the contracting of the service.

Once contracted, the generated QR codes can be monitored and managed from our platform by the client himself, since we will only give technical support. The Information that can be collected or provided by the generated QR codes will be that defined by the client, so it will also be responsible for defining privacy policies harmonized with the GDPR, in case that applies. Mobile Leaves Corp will provide the technical means so that the storage of data is compliance. On the other hand, Mobile Leaves Corp incorporates procedures according to the standard ISO IEC 18004

Here is a detailed description of the technical security measures and organizational implementation, as well as the accredited certifications, which are part of the information provided in our CCT

MOBILE LEAVES CORP has implemented the necessary measures to guarantee the confidentiality, integrity and availability of the data provided by the EXPORTER.

Management of data protection, rights of the interested parties, privacy by design and protection of data regarding employees

Fundamental measures that aim to safeguard the rights of the interested parties, reaction immediate in emergency situations, privacy requirements by design and data protection with respect to employees:

There is an internal data protection management system, the compliance of which is monitored and evaluated constantly on a case-by-case basis and at least every six months.

This internal system is in the process of continuous improvement and includes internal procedures for review and implementation

Among the procedures implemented are the following:

User management procedure: A procedure has been established that aims to detail the system to follow to register an internal user of the system (employees) Through this procedure is assigned to each employee with powers over the processing of personal data a username and password and their access permissions to applications that may contain data from personal character. The user management procedure includes a mapping of the information flow to the who has access, so that it is described who can have access to the information, from what computers you can access and through which applications you can do so. The services contracted to AWS in turn allow us to obtain a history of accesses and to track and monitor the work carried out.

Procedure for managing the rights of interested parties: A procedure has been implemented that allows manage in an agile and simple way any type of request from an interested party (the owner of the data) in consonance with the rights of access, rectification, deletion, opposition, limitation of treatment and portability within the period of one month set by the regulations.

Incident management procedure: A procedure has been developed to identify an incident of a security bankruptcy and to be able to act before them, documenting the entire process. The procedure allows the assessment of the incident, so that its relevance can be calibrated. If the relevance is of the entity, the security bankruptcy management mechanism is activated, informing the EXPORTER of data in a sufficient time to be able to communicate to its Authority of Control the events that occurred.

A policy of non-use of paper documentation is implemented that limits the risks derived from its possible use.

The data is hosted on servers of the AMAZON WEB SERVICES subprocessor, which has, among others, ISO certification in information security systems ISO27001 which gives us to ensure that the necessary technical measures are implemented to ensure availability, integrity and confidentiality of data. The technical details of the security measures implemented and accredited security standards can be found later in this document.

An information procedure has been established for our employees that ensures that they know what are your GDPR rights and obligations

Our privacy policies have been defined so that we can offer legal information transparent to our customers and users, which are updated on our website.

A cookie consent management platform has been implemented for our website, so that their management is GDPR compliance.

Both our website and our servers include encryption systems.

We work with teams with permanently updated operating systems and with updated measures of security, such as antivirus and computer access control by username and password.

In this sense, indicate that the main treatment operations (storage, encryption) are carried out by a subprocessor that complies with the standards of safety and regulatory compliance most recognized worldwide, such as Amazon Web Services.

The contracted services and technical measures implemented are the following:

AWS security and compliance data

Services contracted by Mobile Leaves Corp:

✔EC2

✔RDS in process of change to S3

✔ROUTE 53

✔S3

✔Cloud Trail

Characteristics of each service:

✔EC2 | https://aws.amazon.com/es/ec2/features/

✔RDS | https://aws.amazon.com/en/rds/features/security/

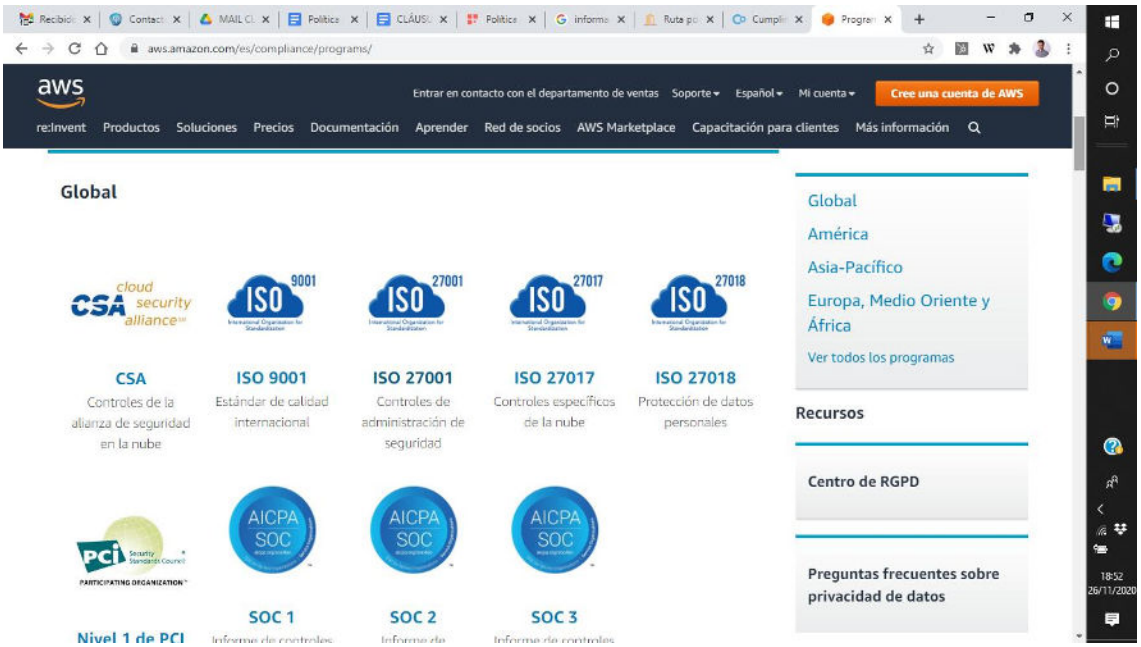
✔ROUTE 53 | https://aws.amazon.com/en/route53/features/

✔S3 | https://aws.amazon.com/es/s3/features/

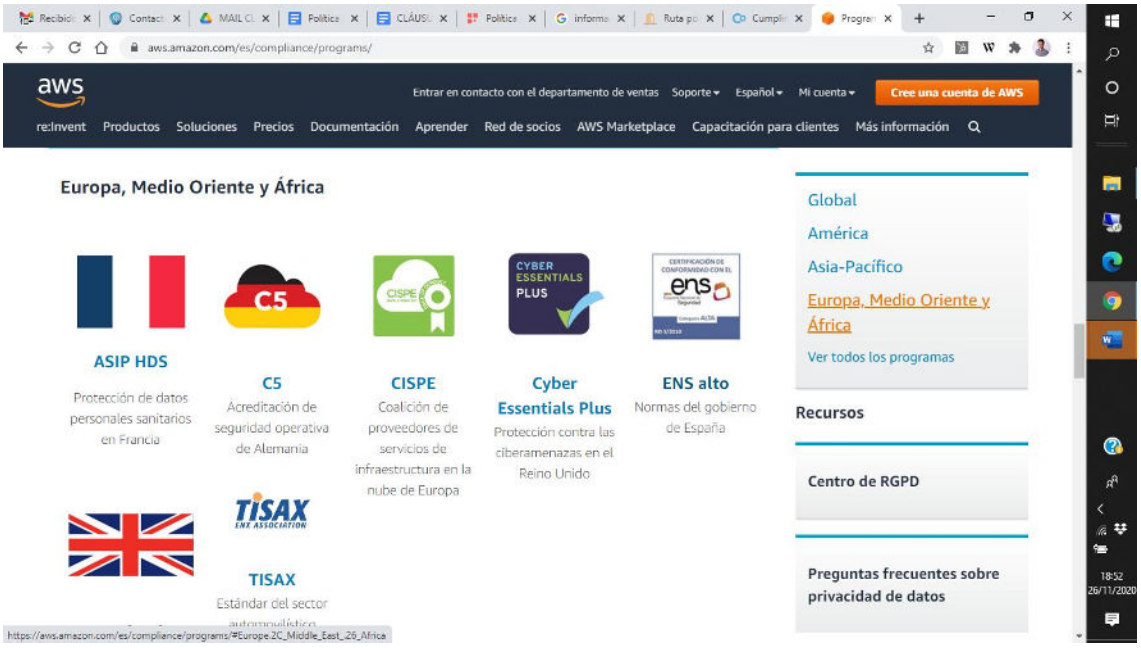
✔CLOUD TRAIL | https://aws.amazon.com/cloudtrail/?nc1=h_ls

MAIN CERTIFICATIONS IN GLOBAL STANDARDS IN SAFETY AND COMPLIANCE AND THAT APPLY TO THE SERVICES CONTRACTED BY MOBILE LEAVES CORP AT A GLOBAL LEVEL

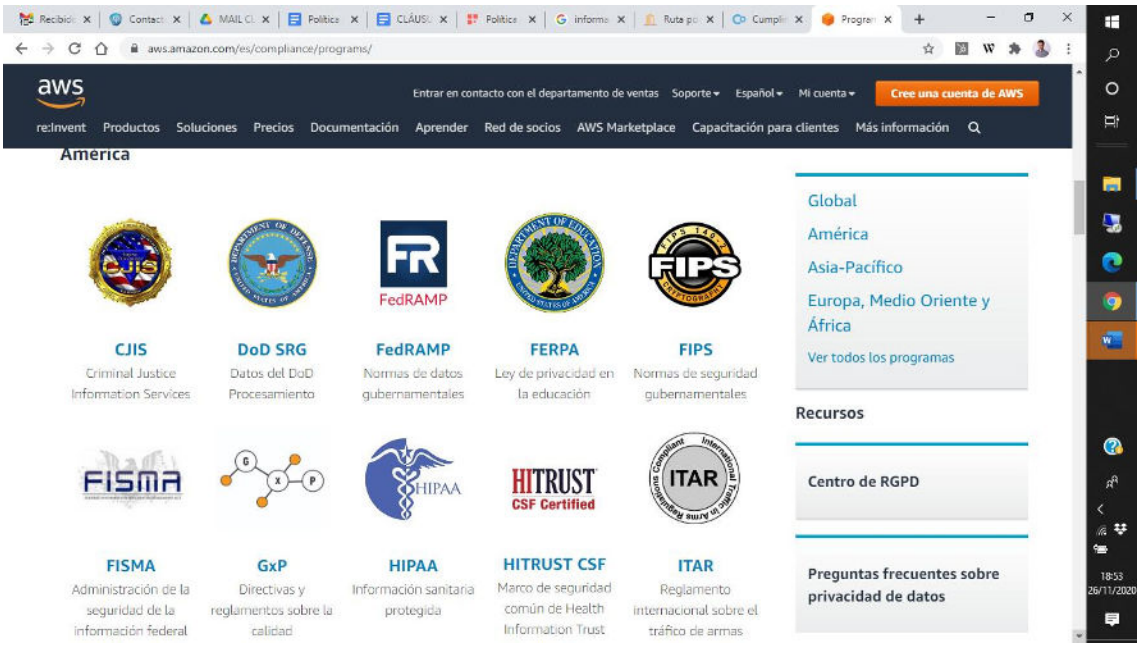
GLOBAL LEVEL



EUROPEAN LEVEL



AMERICA


aws.amazon.com/es/compliance/programs/
aws
Entrar en contacto con el departamento de ventas
Soporte
Español
Mi cuenta
Cree una cuenta de AWS
re:Invent
Productos
Soluciones
Precios
Documentación
Aprender
Red de socios
AWS Marketplace
Capacitación para clientes
Más información
América
CJIS
Criminal Justice Information Services
DoD SRG
Datos del DoD Procesamiento
FedRAMP
Normas de datos gubernamentales
FERPA
Ley de privacidad en la educación
FIPS
Normas de seguridad gubernamentales
FISMA
Administración de la seguridad de la información federal
GxP
Directivas y reglamentos sobre la calidad
HIPAA
Información sanitaria protegida
HITRUST CSF
Marco de seguridad común de Health Information Trust
ITAR
Reglamento internacional sobre el tráfico de armas
Global
América
Asia-Pacífico
Europa, Medio Oriente y África
Ver todos los programas
Recursos
Centro de RGPD
Preguntas frecuentes sobre privacidad de datos