PRIVACY POLICY:

PRIVACY POLICY	
As you are probably aware, the entry into force of (EU) Regulation 2016/679 of the European Parliament and of the Council, of 27th April 2016 on General Data protection (hereinafter GDPR) and Organic Law 3/2018, of 5th December, on Personal Data Protection and Guarantee of Digital Rights (hereinafter OLDPGDR) addresses the need to strengthen the levels of security and protection of personal data. We wish to inform you that we meet all the requirements of this legislation and that all data under our responsibility is processed pursuant to legal requirements and with the due security measures that will guarantee their confidentiality. However, given the legislative changes, we consider it convenient to inform you of the following privacy policy:	
Who is responsible for processing your data?	
Identity:	RAFIA INDUSTRIAL S.A.
Postal address:	CL. LA FABRICA 2 46114 VINALESA (VALENCIA)
Telephone:	961 49 10 81
Email:	gdpr@rafiaindustrial.com
What are your rights?	
• Any person is entitled to obtain confirmation on whether we are processing personal data concerning them, or not.	
• The stakeholders have the right to access their personal data, as well as to request the correction of inaccurate data or, if applicable, request their removal when, among other reasons, the data is no longer necessary for the purposes for which it was collected.	
• It is not possible to exercise the right to correction in the case of video surveillance processing, because given the nature of the data -images taken from the reality that show an objective fact-, this would be a right on content that is impossible to implement.	
• Under certain circumstances, the stakeholder may request limitation of the processing of their data, in which case we will only keep them to place or defend claims.	
• Under certain circumstances and due to reasons pertaining to their particular situation, stakeholders may oppose the processing of their data, in which case the Data Controller will stop processing the data, except for legitimate imperative reasons, or to initiate or defend possible claims. Thus, regarding video surveillance images, exercising the right of opposition entails huge difficulties. If it is interpreted as the impossibility of recording images of a specific subject within the video surveillance installations linked to private security purposes, it would not be possible to satisfy it insofar as protection of safety would prevail.	
• By virtue of the right to portability, the interested parties are entitled to obtain the personal data pertaining to them in a structured and common use format that is mechanically read, and to transfer it to another data controller".	
• In the event that the consent has been given for a specific purpose, you are entitled to withdraw the consent at any time, and this will not affect the legality of the processing based on the consent prior to withdrawing it.	
How can you exercise your rights?	
Where to go to exercise your rights:	"If you wish to exercise your rights, please use the channel established to this purpose by the data controller: gdpr@rafiaindustrial.com so that we may respond to and manage your request"
Information required to exercise your rights:	• In order to exercise your rights, we must verify your identity and the specific request that you are making, therefore we ask for the following information: - Documented information (written/ email) on the request. - Proof of identity as owner of the data object of the request (Name, surnames of the stakeholder and photocopy of the ID of the stakeholder and/or of the person representing them, as well as the document proving said representation (legal representative, if any). - In the event of exercising rights regarding data of deceased persons: Copy of: o Libro de Familia (Family Book) or Civil Registry certification that shows the kinship or relationship to the deceased and/or, o Will that declares the requesting party as the heir and/or, o Express appointment by the deceased of the person or institution requesting the right and/or o Documentation that proves the legal representation of the deceased. o In the event of exercising the right to amendment and/or elimination: A Liability Statement by the requesting party where they prove that they have the consent of the other people linked to the deceased due to kinship or other relationships, as well as the heirs, to make this request. - When the data controller has reasonable doubts on the identity of the individual making the request, they may ask for any additional information that is necessary to confirm the identity of the stakeholder. - Address to purposes of notifications, date and signature of the applicant (if it is in writing), or full name and surnames (if it is by email), or validation of the request in the private area of the communication channel, with the personal code authenticating your identity) • When exercising the right to rectification acknowledged in article 16 of the GDPR, the affected party must state in their request the data in question and the correction to be made. When necessary, they must attach the documentation proving the error or incomplete nature of the data being processed. • Likewise, when a large amount of data pertaining to the affected party is processed and they exercise their right to access, without specifying whether they refer to all or part of the data, the controller may request, prior to providing the information, that the affected party specify the data or processing activity involved in the request.
General Procedure to Exercise your rights:	• Once the required information is received, we will respond to your request pursuant to the organisation's general procedure for exercising rights: • The data controller will provide the stakeholder with information pertaining to their actions based on a request pursuant to articles 15 to 22 (Rights of the stakeholder), and, in any case, within one month from receipt of the request. • This period may be extended another two months, if necessary, taking into account the complexity and the number of requests. • The data controller shall inform the stakeholder of any of these extensions within one month from receipt of the request, stating the reasons for the delay. • When the stakeholder submits the request by electronic means, the information will be provided by electronic means when possible, unless the stakeholder asks that it be provided in another way. • Only in those cases where the controller's processing systems allow, the right to access will be provided through a direct and safe remote access system to the personal data, which will guarantee permanent access to all of the data. To this end, communication by the controller to the affected party of the manner in which they may access this system will suffice to consider the request to exercise their right as satisfied. However, the stakeholder may request from the Data Controller the information referred to in the cases set forth in article 15.1 of the GDPR that is not included in the remote access system.

	• If the data controller does not process the stakeholder's request, they will inform them without delay, and at the latest within one month from receipt of the request, of the reasons for their inaction and that they may submit a claim before a supervising authority and take legal action. • The information provided shall be free of charge, except for reasonable fees for administrative costs. When the affected party chooses a medium other than what is offered to them and that entails a disproportionate cost, the request shall be deemed excessive and therefore the affected party will cover the excess in cost that their choice entails. In this case, the Data Controller shall only be responsible for satisfying the right to access without undue delays. • The data controller may refuse to act on the request; however, they bear the burden of proving the manifestly unfounded or excessive nature of the request. To purposes of the content of article 12.5 of the GDPR, the right to exercise access more than once within a period of six months may be deemed repetitive, unless there is a legitimate reason for it. • In those cases where exercising the right to rectification or elimination are applicable, the data will be blocked: Blocking the data consists of identifying and reserving it, adopting technical and organisational means to prevent its processing, including viewing, except to make it available to judges and courts, the Public Prosecutor Office or the competent Public Administrations, particularly the data protection authorities, for the demand of possible liabilities derived from the processing, and only for the time until they prescribe. After this time, the data will be destroyed. The blocked data may not be processed for any purpose other than that stated above. (Art. 16 GDPR and Art. 32 OLDPGDR) • When the elimination is derived from exercising the right to oppose, according to article 21.2 of the GDPR, the Data Controller may keep the identification data of the affected party that is required in order to prevent future processing for direct marketing purposes. In those cases where you do not wish for your data to be processed to send commercial communication, we remit you to the existing publicity exclusion systems, according to the information published by the competent supervisory authority (AEPD) on its electronic site www.aepd.es • In those cases where personal data processing is limited, it will be clearly shown on the Data Controller's information systems. • When there is a proven, due and payable debt, a communication is sent to the debtor when payment is requested, regarding the possibility of inclusion in said systems (the organisation's debtor processing system), specifying those in which it participates (debt collection agencies to manage the pertinent claim...) if the debt is not resolved within a maximum of 15 days from notification of the insolvency, you are informed of the possibility of exercising the rights established in articles 15 to 22 of the GDPR, within thirty days from notification of the debt to the system, and the data will remain blocked during that time. • People who are related to the deceased through kinship or other relationship, as well as their heirs, may address the data controller or processor in order to request access to their personal data and, where applicable, their correction or elimination. As an exception, the people referred to in the above paragraph may not access the data of the deceased, nor request its correction or elimination, when the deceased had expressly forbidden it or when it is so established by law. This prohibition will not affect the heirs' rights to access the asset data of the deceased. • In order to comply with current regulations on video surveillance Inst 1/2006 of the AEPD, we inform you that the recordings shall be kept for one month from their production, therefore we will not be able to fulfil requests submitted after this period. Also, to prevent third-party rights from being affected, in the event of a request for access, we will issue a certificate that will specify the data that was the object of processing, with the utmost precision possible and without affecting the rights of third parties. For example: "Your image was recorded on our systems on the ___ of the month of the year between _ o'clock and _ o'clock. Specifically, the system records your access and exit from the facilities."
What are the methods for placing a claim?	
If you believe that your rights were not duly taken care of, you are entitled to submit a claim before the competent data protection authority (www.agpd.es)	

ADDITIONAL INFORMATION CONTACT DATA PROCESSING:

What is the purpose of processing the personal data that you provide to us? (*) The list of RAFIA INDUSTRIAL S.A.'s activities is available at www.rafiaindustrial.com
• Replies to your questions and requests: To manage Replies to Questions, Claims or Incidents, Requests for technical or corporate information, Resources and/or Activities and, if you provided consent, to the purposes described in the additional consent.
• Contact with the stakeholder via the media provided (email, postal address and/or phone number) in order to manage the questions you ask us through the channels established to this purpose, manage notifications and coordinate actions derived from the services requested by people related with RAFIA INDUSTRIAL S.A. and/or by data processors involved with it to the approved and/or allowed purposes.
• Management of inscriptions for RAFIA INDUSTRIAL S.A. conferences and events
• Management of subscriptions to the RAFIA INDUSTRIAL S.A. newsletter.
• Contact and/or sending out of satisfaction surveys, newsletters and corporate information and offers and promotions on the organisation's products and services.
• Recording and subsequent publication of audiovisual and/or graphic material in which you may be involved in corporate communication media (for example, but not limited to, website, social media, newsletters, activity report, news items, presence in the media) and/or other public communication media (industry publications and/or reports in the press, TV, etc.) as publication of the results of the activity, promotion and dissemination, campaign management, activities and events, if you provided consent.
• Associated processing, including its prior communication, that may be derived from the performance of any operation for structural modification of companies or the provision or transfer of business or of a branch of corporate activity, provided that the processing is necessary to the proper completion of the operation and that it guarantees, where applicable, continuity in the provision of services.
• Inclusion in the reporting channel systems of the data associated to the disclosure (including anonymously) of the commission, within the organisation or within the actions of third-parties contracting with it, of actions or conducts that may be contrary to applicable general or industry regulations.
How long do we keep the data provided?
• The data provided will be kept as long as the legality of processing remains, and once it is expired, until the stakeholder requests its elimination, except for its conservation to formulate, exercise or defend claims by the data controller, or with the aim to protect the rights of other individuals or entities and/or for legally mandatory reasons. • The data processed in order to send commercial communications will be kept until the consent given is revoked. • The data of the person communicating a complaint and of the employees and third-parties is kept in the complaints system to decide on whether an investigation should be proceeded with on the reported facts, as well as subsequently as evidence of the operation of the model to prevent crime by the entity, according to article 24 of the OLDPGDR.
What is the legal basis for processing your data?
• The legal basis for processing your data is to fulfil your request from us. The requested data is necessary for the proper fulfilment of the service. • To satisfy a legitimate interest of the Controller: Cases of legitimate interest where the controller may be the injured party and it were necessary to process and notify the data of the breaching party to third parties, to ensure observance of regulations and defence of the interest of the data controller, as well as cases of legitimate interest in specific processing as contemplated in the OLDPGDR: Article 19. Contact data and individual employer data processing; Article 20. Credit information systems; Article 21. Processing related to the performance of certain business operations (company restructuring or business transfers) Article 22. Processing to purposes of video surveillance; Article 23. Publicity exclusion systems; Article 24. Internal complaint information systems).

• Consent of the stakeholder who has unequivocally provided it to use through formal means and/or by checking the boxes provided to said purpose in the data protection clauses contained in the basic document regulating the commercial relationship, depending on the contact channel.
Who can your data be communicated to?
• Organisations or individuals directly hired by the Data Controller to provide services connected to the processing purposes: Collaborators, Organisations Subcontracted to perform projects/services object of request or consultation. • Complaints Channel (Complaints on the breach of regulations and code of conduct are forwarded to the Regulation Compliance Unit): Access to the data contained in these systems will be limited exclusively to those who, integrated or not within the organisation, perform internal monitoring and compliance duties, or to the data processors that are eventually appointed to this purpose. However, access by other people, or even communication to third parties, will be legal when it is necessary in order to take disciplinary action or to follow the legal proceedings that are necessary, when applicable. • Law Enforcement and Safety Agencies: To the extent required, a proven right to access within the investigation of a breach of regulations. • Others (specify): Media and specialised journals to promote the organisation's activities.
Under what guarantee is your data communicated?
Data is communicated to third parties who prove that they have a Personal Data Protection System pursuant to current legislation.
How did we obtain your data?
• From the stakeholder themselves, through communication sent and/or through professional social media.
What type of data do we process?
Identification and contact data, data related to and/or provided with the question, request for technical or corporate information, resources and/or activities, claims lodged or incidents notified to us, as well as the personal data of third parties that may be provided.
How is your personal data safely stored?
RAFIA INDUSTRIAL S.A. has formalised agreements to guarantee that we process your personal data correctly and pursuant to current data protection regulations. These agreements contain the respective duties and responsibilities towards you, and they contemplate which entity is best positioned to fulfil your needs. These agreements do not affect your rights by virtue of the data protection law. Please contact us if you wish to obtain further information on these agreements. The Data Controller takes all the steps required to keep your personal data private and safe. Only authorised RAFIA INDUSTRIAL S.A. staff, authorised staff of third parties directly hired by the Data Controller to perform services linked to the processing purposes, or authorised staff with companies that invoice under the commercial name of RAFIA INDUSTRIAL S.A.* (that have the legal and contractual obligation to keep all of the information safe) have access to your personal data. All of the RAFIA INDUSTRIAL S.A. staff who have access to your personal data is required to undertake to observe the Data Controller Privacy Policy and the data protection regulations, and all third-party employees who have access to your personal data must sign the confidentiality agreements under the terms established by current legislation. In addition, third-party companies who have access to your personal data are bound by contract to store your data safely. To ensure that your personal data is protected, RAFIA INDUSTRIAL S.A. has an IT safety environment and takes the necessary measures to prevent non-authorised access. The Data Controller has formalised agreements to guarantee that we process your personal data correctly and pursuant to current data protection regulations. These agreements contain the respective duties and responsibilities towards you, and they contemplate which entity is best positioned to fulfil your needs. These agreements do not affect your rights by virtue of the data protection law. Please contact us if you wish to obtain further information on these agreements.

ADDITIONAL INFORMATION CLIENT DATA PROCESSING:

What is the purpose of processing your personal data? (*) The list of RAFIA INDUSTRIAL S.A.'s activities is available at www.rafiaindustrial.com
• Internal use, commercial and relation management. Operations and administrative, economic and accounting management derived from relations with the client and/or debtor
• Internal use, administrative, economic and accounting operations and management derived from relations with the assignor (commercial and/or contractual relations)
• Commercial offers and management from the organisation and its services "With the purpose to provide offers of services that may be of your interest"
• Commercial offers and management by RAFIA INDUSTRIAL S.A. and its services "With the purpose to provide offers of services that may be of your interest"
• Contract management and provision of services by the organisation, as well as fulfilment of contract requirements
• Management of Replies to Questions, Claims or Incidents, Requests for Information, Resources and/or Activities
• Promotion and Information on the Organisation: The Production, Publication and Communication of Statistics, Activity Logs, Success Stories and Information associated with the communication and transparency of their Activity, as well as the Recording and Publication of Informational Material, Communication and Management of Campaigns, Activities, Events, Competitions and/or Recording and Publication, in the organisation's media (including website and social media) and/or other public communication media, of videos, recordings and photos associated with the activities carried out by the organisation "In order to provide stakeholders with information on the organisation"
• Sending out of Newsletters, Activity Reports and Information associated with the Organisation's Activities
• Quality Assurance of processes and activities, as well as the assessment of satisfaction/perception results and performance by the organisation stakeholders.
• Provision of proof of technical solvency in the submission of tenders and/or request, management and justification of campaigns, activities, events, tenders, projects and grants where the organisation participates
• Management of Regulation Compliance (applicable regulations as well as mandatory internal regulations): Investigation, monitoring and audit of controls established to prevent crime with the possibility of establishing controls at the facilities access, information and document printing systems for all personal data that is under the responsibility of the organisation and therefore for all of the company's information systems, as well as controls pertaining to the use of the images recorded by the video surveillance systems to investigate accidents and/or incidents that may happen, as well as breaches of labour regulations, crimes or illegal conducts.
• Profile Analysis "In order to offer you products and services tailored to your interests, as well as to improve your customer experience, we will produce a "profile" based on the information provided. No automated decisions will be taken based on this profile".
• Assessment of Asset Solvency and Credit
• Contacts / Agenda management
• Statistical, historical or scientific purposes
• Management of Visits and Video Surveillance of the Facilities, as well as of safety and compliance with regulations, investigation of possible incidents or accidents, management of associated insurance and of warnings or penalties due to breach of safety regulations.

- Management and auditing of quality, environmental management and/or management of occupational safety regarding organisation processes and facilities.
- Check on the publicity exclusion systems that may affect their activity, excluding from processing the data of the parties who have expressed their opposition or refusal to processing by checking the publicity exclusion systems published by the competent supervisory authority.
- Associated processing, including its prior communication, that may be derived from the performance of any operation for structural modification of companies or the provision or transfer of business or of a branch of corporate activity, provided that the processing is necessary to the proper completion of the operation and that it guarantees, where applicable, continuity in the provision of services.
- Inclusion in the reporting channel systems of the data associated to the disclosure (including anonymously) of the perpetration, within the organisation or within the actions of third-parties contracting with it, of actions or conducts that may be contrary to applicable general or industry regulations.
- Others (specify): In the event of deposit contracts, RAFIA INDUSTRIAL S.A. reserves the right to carry out regular audits at client and other debtor facilities.

How long do we keep your data?

- The data provided will be kept as long as the legality of processing remains, until the stakeholder requests its elimination after the relation with the stakeholder has finished in writing, except for its conservation to formulate, exercise or defend claims by the data controller, or with the aim to protect the rights of other individuals or entities and/or for legally mandatory reasons.
- In any case, when the relationship is finalised, the data of the stakeholder will be duly blocked, pursuant to current data protection regulations.
- Accounting and Tax Documentation - To tax purposes: The accounting books and other mandatory logs required by the pertinent tax regulations (Withholdings, VAT, Corporate Tax, etc.) as well as the documentation proving the annotations recorded in the books (including the computer programs and files and any other proof that is relevant to taxes), must be kept at least for the time in which the Government is entitled to check and investigate and, consequently, to settle tax debts (Articles 66 to 70 of the General Tax Law). Prescription period for Tax Offences associated with verification of the tax base or fees compensated or pending compensation or of deductions applied or pending application and to Offences against the Tax Authorities and the Social Security - Art. 66 bis General Tax Law and Criminal Procedure Code, respectively. - 4 years. Prescription of offences 10 years.
- Accounting and Tax Documentation - To corporate purposes: Books, correspondence, documentation and proof concerning your business, duly organised starting from the latest inscription made in the books, unless otherwise established by general or special provisions. This commercial obligation applies both to the mandatory books (income, expenditures, investment assets and provisions), as well as the documentation and proof for the annotations recorded in the books (invoices issued and received, tickets, corrective invoices, bank documents, etc.) (Art. 30 of the Commerce Code) - 6 years.
- Solvency files: Data pertaining to regular, due and payable and non-claimed debts (Art. 20 of the OLDPGDR) - as long as the breach persists, with a maximum limit of five years from the due date of the money, financial or credit liability – 5 years.
- The images/sounds recorded by the video surveillance systems will be eliminated within a maximum period of one month from their recording, except if they have to be kept to prove the perpetration of acts that threaten the integrity of people, assets or facilities (in which case the images will be made available to the competent authorities within a maximum period of 72 hours from when the existence of the recording was known), or if they are related to serious or very serious criminal or administrative offences regarding public safety, with an ongoing police investigation or with ongoing legal or administrative proceedings (Instruction 1/2006 of 8 November, of the AEPD, on personal data processing to purposes of surveillance via camera or video camera systems and Art. 22 OLDPGDR) - 30 days.
- The data included in the automated files created to monitor access to buildings (Instruction 1/1996, of 1 March, of the AEPD, on automated files established with the purpose to monitor access to buildings) - 30 days.
- Data processed regarding the legal guarantee will be kept during the lifetime of the legal guarantee and once it expires, for the period in which there may be a legal or administrative claim pertaining to the legal guarantee.
- The data processed in order to send commercial communications will be kept until the consent given is revoked.
- The data of the person communicating a complaint and of the employees and third-parties are kept in the complaints system to decide on whether an investigation should be proceeded with on the reported facts, as well as subsequently as evidence of the operation of the model to prevent crime by the entity, according to article 24 of the OLDPGDR.
- Therefore, the data will be kept as long as the commercial relationship continues, based on the conservation timeframes established by current regulations, as well as the timeframes legally or contractually established for the implementation or prescription of any liability action due to breach of contract by the stakeholder or by the Organisation (reform of the Civil Code establishes a period of five years to take action for civil liability, which begins from the date when fulfilment of the obligation may be demanded).

What is the legal basis for processing your data?

- The legal basis for processing your data is the execution of a contract: fulfilment of your request, offer, order and/or business contract, to which end the data provided will be notified to the person in charge of the Brand so that they may properly manage, where applicable, the warranties and liabilities of the products and services they provide. The requested data is necessary for the proper fulfilment of the service.
- Fulfilment of legal obligations: Regulations with the status as administrative, commercial, tax, fiscal, accounting and financial law and legislation to defend consumers and users.
- To satisfy a legitimate interest of the Controller: Data processing as part of a commercial relationship and/or contract, that is required for its maintenance or fulfilment; transfer of data within corporate groups to internal administrative purposes, direct marketing, fraud prevention, cases of legitimate interest where the controller may be the harmed party and the data of the breaching party has to be processed and notified to third parties in order to manage regulation compliance and to defend the interests of the data controller; to purposes of video surveillance as legitimate interest of the organisation to protect its assets; the legitimate interest of direct marketing implemented by the LSSICE (sending commercial communications regarding products or services similar to those contracted by the client with whom there is a prior contractual relationship), as well as in cases of legitimate interest of specific processing contemplated in the OLDPGDR: Article 19. Contact data and individual employer data processing; Article 20. Credit information systems; Article 21. Processing related to the performance of certain business operations (company restructuring or business transfers) Article 22. Processing to purposes of video surveillance; Article 23. Publicity exclusion systems; Article 24. Internal complaint information systems).
- Consent of the stakeholder who has unequivocally provided it to use through formal means and/or by checking the boxes provided to said purpose in the data protection clauses contained in the basic document regulating the commercial relationship, depending on the commercial contact channel.

Who can your data be communicated to?

- Organisations or individuals directly hired by the Data Controller to provide services connected to the processing purposes (specify): Companies belonging to the Group (see list at www.armandoalvarez.com), Commercial agents and/or agencies, companies related to management of transportation, publicity/marketing agencies, legal consultancies, organisations subcontracted to perform work/services object of the contract with the client, collection management and credit insurance organisations, management and/or regulation compliance auditors.
- Public Administration organisations or agencies with competences in the matters object of the processing (specify): AEAT (Spanish Tax Agency)
- Financial organisations (specify): Bank standing orders and/or management of collections of instruments and other means of payment.
- Law Enforcement and Safety Agencies (specify): To the extent required, a proven right to access within the investigation of a breach of regulations.
- Compliance Complaints Channel (Complaints on the breach of regulations and code of conduct are forwarded to the Regulation Compliance Unit): Access to the data contained in these systems will be limited exclusively to those who, integrated or not within the organisation, perform internal monitoring and compliance duties, or to the data processors that are eventually appointed to this purpose. However, access by other people, or even communication to third parties, will be legal when it is necessary in order to take disciplinary action or to follow the legal proceedings that are necessary, when applicable.

• Others (specify): Media and specialised journals to promote the organisation's activities.
Under what guarantee is your data communicated?
Data is communicated to third parties who prove that they have a Personal Data Protection System pursuant to current legislation.
How did we obtain your data?
• The stakeholder themselves or their legal representative
• Private organisation (specify): Other Companies belonging to the Group, commercial agents, as well as the Organisation with which the controller has a contractual or service provision relation and to which end they must have the personal data of contact people for administrative and operational management in order to manage their access, inclusion in the intended project/service and/or verification of compliance with regulations under the responsibility of the organisation.
What type of data do we process?
Identification data of Potential and Effective Clients, contact persons for administrative and operative management associated to the implementation of the contract/project, as well as other debtors from commercial transactions; data pertaining to the position of contact persons for administrative and operative management associated to the implementation of the contract/project; commercial information; economic, financial and/or payment conditions data; other type of data (specify): Name, surnames and Tax ID of the legal representative, contact information for people in the organisation involved with or related to the project object of the contract/order.
How is your personal data safely stored?
Regarding the processing of your personal data, we inform you: RAFIA INDUSTRIAL S.A. takes all the steps required to keep your personal data private and safe. Only authorised RAFIA INDUSTRIAL S.A. staff, authorised staff of third parties directly hired by the Data Controller to perform services linked to the processing purposes, or authorised staff with companies that invoice under the commercial name of RAFIA INDUSTRIAL S.A. (that have the legal and contractual obligation to keep all of the information safe) have access to your personal data. All of the RAFIA INDUSTRIAL S.A. staff who have access to your personal data is required to undertake to observe the Data Controller Privacy Policy and the data protection regulations, and all third-party employees who have access to your personal data must sign the confidentiality agreements under the terms established by current legislation. In addition, third-party companies who have access to your personal data are bound by contract to store your data safely. To ensure that your personal data is protected, RAFIA INDUSTRIAL S.A. has an IT safety environment and takes the necessary measures to prevent non-authorised access. The Data Controller has formalised agreements to guarantee that we process your personal data correctly and pursuant to current data protection regulations. These agreements contain the respective duties and responsibilities towards you, and they contemplate which entity is best positioned to fulfil your needs. These agreements do not affect your rights by virtue of the data protection law. Please contact us if you wish to obtain further information on these agreements. **Regarding the personal data that** RAFIA INDUSTRIAL S.A. **may have access to as consequence of the contracted services, we inform you:** The provision of services object of the contract may entail physical access by RAFIA INDUSTRIAL S.A. staff to premises or facilities that may store personal data for which the client is the data controller. To this purpose, RAFIA INDUSTRIAL S.A. has signed with its staff clauses that forbid access to any type of confidential information and, specifically, to personal data belonging to the client, unless the service contemplates within its scope the transfer, repair, destruction and/or management of computer hardware that may contain personal data. In this case RAFIA INDUSTRIAL S.A. would act as the data processor, establishing in this case the pertinent contract according to current regulations on data protection that would contemplate, among other aspects, the object, duration, nature, purpose, category of the data object of the processing, safety measures, the controller's obligations and rights, organisation and technical safety measures to guarantee confidentiality during the process, as well as the agreements reached between the client and the processor regarding the transmission of safety breaches and/or exercise of rights. If the client does not formalise the personal data processing service in a contract, it entails that RAFIA INDUSTRIAL S.A. has no associated liability as the data processor. Notwithstanding the above, if they learn of any type of confidential information with the object of providing the service, they undertake to keep it secret, not to disclose or publicise it, either directly or through third parties or companies, and to not make it available to third parties. This confidentiality obligation is indefinite, and will persist after the contract is terminated for any reason. RAFIA INDUSTRIAL S.A. undertakes to communicate and to enforce for its staff and the persons hired by it the established obligations regarding confidentiality.

ADDITIONAL INFORMATION SUPPLIER DATA PROCESSING:

What is the purpose of processing your personal data? (*) The list of RAFIA INDUSTRIAL S.A.'s activities is available at www.rafiaindustrial.com
• Internal use, commercial and relation management. Operations and administrative, economic and accounting management derived from relations with the supplier/collaborator.
• Internal use, administrative, economic and accounting operations and management derived from relations with the assignor (commercial and/or contractual relations)
• Contract management and provision of services by the organisation, as well as fulfilment of contract requirements.
• Management of Replies to Questions, Claims or Incidents, Requests for Information, Resources and/or Activities.
• Promotion and Information on the Organisation: The Production, Publication and Communication of Statistics, Activity Logs and Information associated with the communication and transparency of the Activity, as well as the Recording and Publication of Informational Material, Communication and Management of Campaigns, Activities, Events, Competitions and/or Recording and Publication, in the organisation's media (including website and social media) and/or other public communication media, of videos, recordings and photos associated with the activities carried out by the organisation that may contain people in the performance of their duties "With the purpose to provide stakeholders with information on the organisation".
• Sending out of Newsletters, Activity Reports and Information associated with the Organisation's Activities.
• Quality Assurance of processes and activities, as well as the assessment of satisfaction/perception results and performance by the organisation stakeholders.
• Management of the Selection, Certification and Hiring of Suppliers/Collaborators and verification of compliance with regulations
• Health and safety management (occupational hazard prevention and safety monitoring) and evaluation of compliance
• Management of submission of technical solvency in the submission of tenders and/or request, management and justification of campaigns, activities, events, tenders, projects and grants where the organisation participates.
• Monitoring of working hours and/or presence or attendance and of performance
• Management of Regulation Compliance (applicable regulations as well as mandatory internal regulations): Investigation, monitoring and audit of controls established to prevent crime with the possibility of establishing controls at the facilities access, information and document printing systems for all personal data that is under the responsibility of the organisation and therefore for all of the company's information systems, as well

as controls pertaining to the use of the images recorded by the video surveillance systems to investigate accidents and/or incidents that may happen, as well as breaches of labour regulations, crimes or illegal conducts.

- Contacts/Agenda management
- Statistical, historical or scientific purposes
- Access control and video surveillance of the facilities, as well as safety and regulation compliance in them, to keep the people, goods and installations safe, as well as to perform duties to monitor workers as established in article 20.3 of the Workers' Statute, investigation of possible incidents or accidents, manage associated insurance and manage warnings or penalties due to breaches of safety regulations.
- Management and auditing of quality, environmental management and/or management of occupational safety regarding organisation processes and facilities.
- Associated processing, including its prior communication, that may be derived from the performance of any operation for structural modification of companies or the provision or transfer of business or of a branch of corporate activity, provided that the processing is necessary to the proper completion of the operation and that it guarantees, where applicable, continuity in the provision of services.
- Inclusion in the reporting channel systems of the data associated to the disclosure (including anonymously) of the perpetration, within the organisation or within the actions of third-parties contracting with it, of actions or conducts that may be contrary to applicable general or industry regulations.
- Other: RAFIA INDUSTRIAL S.A. reserves the right to carry out regular audits at client and creditor facilities.

How long do we keep your data?

- The data provided will be kept as long as the legality of processing remains, until the stakeholder requests its elimination after the relation with the stakeholder has finished in writing, except for its conservation to formulate, exercise or defend claims by the data controller, or with the aim to protect the rights of other individuals or entities and/or for legally mandatory reasons.
- In any case, when the relationship is finalised, the data of the stakeholder will be duly blocked, pursuant to current data protection regulations.
- Accounting and Tax Documentation - To tax purposes: The accounting books and other mandatory logs required by the pertinent tax regulations (Withholdings, VAT, Corporate Tax, etc.) as well as the documentation proving the annotations recorded in the books (including the computer programs and files and any other proof that is relevant to taxes), must be kept at least for the time in which the Government is entitled to check and investigate and, consequently, to settle tax debts (Articles 66 to 70 of the General Tax Law). Prescription period for Tax Offences associated with verification of the tax base or fees compensated or pending compensation or of deductions applied or pending application and to Offences against the Tax Authorities and the Social Security - Art. 66 bis General Tax Law and Criminal Procedure Code, respectively. - 4 years. Prescription of offences 10 years.
- Accounting and Tax Documentation - To corporate purposes: Books, correspondence, documentation and proof concerning your business, duly organised starting from the latest inscription made in the books, unless otherwise established by general or special provisions. This commercial obligation applies both to the mandatory books (income, expenditures, investment assets and provisions), as well as the documentation and proof for the annotations recorded in the books (invoices issued and received, tickets, corrective invoices, bank documents, etc.) (Art. 30 of the Commerce Code) – 6 years.
- Occupational Hazard Prevention documentation - Documentation on information and training for employees. Files on occupational accidents or professional illnesses (Legislative RD 5/2000, dated 4 August, approving the consolidated text of the Law on Offences and Penalties in the Social Order) – 5 years.
- The images/sounds recorded by the video surveillance systems will be eliminated within a maximum period of one month from their recording, except if they have to be kept to prove the perpetration of acts that threaten the integrity of people, assets or facilities (in which case the images will be made available to the competent authorities within a maximum period of 72 hours from when the existence of the recording was known), or if they are related to serious or very serious criminal or administrative offences regarding public safety, with an ongoing police investigation or with ongoing legal or administrative proceedings (Instruction 1/2006 of 8 November, of the AEPD, on personal data processing to purposes of surveillance via camera or video camera systems and Art. 22 OLDPGDR) - 30 days.
- The data included in the automated files created to monitor access to buildings (Instruction 1/1996, of 1 March, of the AEPD, on automated files established with the purpose to monitor access to buildings) - 30 days.
- Data processed regarding the legal guarantee will be kept during the lifetime of the legal guarantee and once it expires, for the period in which there may be a legal or administrative claim pertaining to the legal guarantee.
- Solvency files: Data pertaining to regular, due and payable and non-claimed debts (Art. 20 of the OLDPGDR) - as long as the breach persists, with a maximum limit of five years from the due date of the money, financial or credit liability – 5 years.
- The data processed in order to send commercial communications will be kept until the consent given is revoked.
- The data of the person communicating a complaint and of the employees and third-parties are kept in the complaints system to decide on whether an investigation should be proceeded with on the reported facts, as well as subsequently as evidence of the operation of the model to prevent crime by the entity, according to article 24 of the OLDPGDR.
- Therefore, the data will be kept as long as the commercial relationship continues, based on the conservation timeframes established by current regulations, as well as the timeframes legally or contractually established for the implementation or prescription of any liability action due to breach of contract by the stakeholder or by the Organisation (reform of the Civil Code establishes a period of five years to take action for civil liability, which begins from the date when fulfilment of the obligation may be demanded).

What is the legal basis for processing your data?

- Performance of a contract: To fulfil the proposal, order and/or commercial contract.
- To fulfil a legal obligation: Regulations with the status as administrative, commercial, tax, fiscal, accounting and financial law, law on occupational hazard prevention, social security and applicable industry regulations.
- To satisfy a legitimate interest of the Controller: Data processing as part of a commercial relationship and/or contract, that is required for its maintenance or fulfilment; transfer of data within corporate groups to internal administrative purposes, fraud prevention, as well as cases of legitimate interest where the controller may be the harmed party and the data of the breaching party has to be processed and notified to third parties in order to manage regulation compliance and to defend the interests of the data controller; to purposes of video surveillance as legitimate interest of the organisation to protect its assets; as well as in cases of legitimate interest of specific processing contemplated in the OLDPGDR: Article 19. Contact data and individual employer data processing; Article 20. Credit information systems; Article 21. Processing related to the performance of certain business operations (company restructuring or business transfers) Article 22. Processing to purposes of video surveillance; Article 24 Internal complaint information systems).
- Consent of the stakeholder who has unequivocally provided it to use through formal means and/or by checking the boxes provided to said purpose in the data protection clauses contained in the basic document regulating the commercial relationship, depending on the contact channel.

Who can your data be communicated to?

- Organisations or individuals directly hired by the Data Controller to provide services connected to the processing purposes: Companies belonging to the Group (see list at www.armandoalvarez.com), Legal Consultancy, Management and/or Regulation Compliance Auditors, Prevention Services, third parties that are provided with subcontractor employee data for them to access the facilities.
- Public Administration organisations or agencies with competences in the matters object of the processing: AEAT (Spanish Tax Agency)
- Financial institutions: Transfer and/or management of payment instruments.

- Labour Unions, Staff Meetings/Workers' Committee: Employee representatives: Contractors or subcontractors as established (including self-employed persons) (article 35.2 CC and article 42 ET): Tax ID, corporate name, corporate address, object of the contract, Social Security employer inscription number, place where the contract is implemented, coordination of activities from the standpoint of workplace hazards, estimated duration of the contract (initial and completion date). Number of workers who will be employed by the contractor or subcontractor at the main company's workplace.
- Compliance Complaints Channel (Complaints on the breach of regulations and code of conduct are forwarded to the Regulation Compliance Unit): Access to the data contained in these systems will be limited exclusively to those who, integrated or not within the organisation, perform internal monitoring and compliance duties, or to the data processors that are eventually appointed to this purpose. However, access by other people, or even communication to third parties, will be legal when it is necessary in order to take disciplinary action or to follow the legal proceedings that are necessary, when applicable.
- Hazard Prevention Agents are authorised to access the information and documentation pertaining to the work conditions that are necessary to perform their duties and, particularly, that set forth in articles 18, 23 and 36 of the LPRL. The content of section 2 of article 65 of the Workers' Statute regarding due professional secrecy on information they have access to thanks to their work with the company shall apply to the Prevention Agents. (Article 37.3 LPRL).
- Occupational Hazard Prevention Services: the processing by the occupational hazard prevention services of the medical history, due to the medical check-ups performed on the employees, shall be limited to the content of article 22.4 of the LPRL. Thus, access to the medical information obtained under the content of the LPRL by the employer or any third party is forbidden, including persons or agencies with responsibilities on prevention, other than the "medical staff and health authorities who monitor the employees' health", with the sole exception of the conclusions derived from said monitoring regarding the capacity of the workers to perform their job.

Under what guarantee is your data communicated?

Data is communicated to third parties who prove that they have a Personal Data Protection System pursuant to current legislation.

How did we obtain your data?

- The stakeholder themselves or their legal representative
- Other Group Companies, as well as the organisation with which the controller has a contractual or service provision relation and to which end they must have the personal data of contact people for administrative and operational management in order to manage their access, addition to the intended project/service and/or verification of compliance with regulations under the responsibility of the organisation (e.g. data on workers who are going to perform the contracted jobs in terms of coordination of company activities associated with the prevention of occupational hazards).

What type of data do we process?

Trade data, of contact persons for the administrative and operational management associated with the performance of the contract/project and of workers who are going to perform the contracted jobs in terms of coordination of company activities associated with the prevention of occupational hazards; As consequence of the submission of CVs of the supplier's staff involved in the provision of the service/work, in order to prove technical solvency in tenders; In the event of staff who will perform the contracted jobs in terms of coordination of company activities associated with the prevention of occupational hazards (The data that may be derived from possible workplace incidents or accidents by subcontract workers would be contained in the "Occupational Hazard Prevention" processing); Licenses or certifications, in the case of workers who are going to perform the contracted jobs in terms of coordination of company activities associated with the prevention of occupational hazards; Professional details and employment details as consequence of the provision of CVs of the supplier's staff involved in the provision of the service/work, in order to prove technical solvency in tenders; Commercial information and certification data; Data on economic, financial and/or collection conditions; Goods and services provided by the affected party, Financial operations; Other type of data: Name, surnames and Tax ID of the legal representative, contact information for people in the organisation involved with or related to the project object of the contract/order.

The data structure that we process does not contain data pertaining to sentences and criminal offences, nor sensitive data, except in those cases where the holder has special conditions and has to provide documentation that contains said information in order to be accredited or to prove compliance with said condition.

How is your personal data safely stored?

RAFIA INDUSTRIAL S.A. takes all the steps required to keep your personal data private and safe. Only persons authorised by RAFIA INDUSTRIAL S.A., authorised third-party employees or authorised staff of our companies (who have the legal and contractual obligation to store all the information safely) have access to your personal data. All of the RAFIA INDUSTRIAL S.A. staff who have access to your personal data is required to undertake to observe the RAFIA INDUSTRIAL S.A. Privacy Policy and the data protection regulations, and all third-party employees who have access to your personal data must sign the confidentiality agreements under the terms established by current legislation. In addition, third-party companies who have access to your personal data are bound by contract to store your data safely. To ensure that your personal data is protected, RAFIA INDUSTRIAL S.A. has an IT safety environment and takes the necessary measures to prevent non-authorised access.

RAFIA INDUSTRIAL S.A. has formalised agreements to guarantee that we process your personal data correctly and pursuant to data protection legislation. These agreements contain the respective duties and responsibilities towards you, and they contemplate which entity is best positioned to fulfil your needs. These agreements between companies of the group do not affect your rights by virtue of the data protection law. Please contact us if you wish to obtain further information on these agreements.

CONFIDENTIALITY AND INFORMATION TO THIRD PARTIES FOR WHICH YOU PROVIDE US DATA

In compliance with the personal data protection regulations, we process the information that you provide to us (as well as the personal data of contact persons for administrative and operative management in order to manage your access, incorporation to the project/service object of the contracted service and/or verification of regulation compliance under the responsibility of the organisation, personal data of the entity's legal representatives and/or of the people involved in the project (CV) and/or personal references from prior jobs in order to prove technical solvency and, where applicable, personal data regarding staff who will perform the work contracted in terms of corporate activity coordination associated with occupational hazard prevention) as established in the clause and additional information on data protection.

With the acceptance and/or validation of the process that is the basis for the formalisation of your relationship with RAFIA INDUSTRIAL S.A., you expressly consent to the data processing in accordance with the clause and additional information on data protection, as well as to informing and having the consent from third parties of those whose personal data you provide to us for said processing. Additionally, and as long as that as consequence of your relationship with RAFIA INDUSTRIAL S.A. you may have access to personal data and/or confidential information, you undertake to maintain absolute confidentiality and discretion on the information obtained on the activities, interested parties and organisations related to RAFIA INDUSTRIAL S.A., especially regarding Personal Data, even after termination of your relationship with the organisation.

As stated above, you undertake to inform, expressly, precisely and unequivocally, in name and on behalf of RAFIA INDUSTRIAL S.A., the owners of the data of those who provide information to RAFIA INDUSTRIAL S.A. -within a month of the data being notified to RAFIA INDUSTRIAL S.A., of the following aspects *"Your personal data will be communicated to the Data Controller* RAFIA INDUSTRIAL S.A. -gdpr@rafiaindustrial.com *and monitor compliance with applicable legislation relating to the staff appointed by the supplier/ collaborator to perform the job hired by* RAFIA INDUSTRIAL S.A. *and to maintain a history of business relations. This processing is mandatory pursuant to current legislation. The refusal to provide the data to* RAFIA INDUSTRIAL S.A. *may entail the termination of the contract. The stakeholder is also informed that, in accordance with current legislation,* RAFIA INDUSTRIAL S.A. *must communicate the information and data collected during the hiring process to agencies and third parties to whom* RAFIA INDUSTRIAL S.A. *is obligated to inform of this data by virtue of current regulations.* ***Rights****: The stakeholder may access, correct and eliminate the data, as well as limit, withdraw or oppose its processing, by following the procedures established in our privacy policy. If you deem that the exercise of your rights was not fully satisfactory, you may submit a claim with the national supervisory authority by addressing the Spanish Data Protection Agency, C/Jorge Juan, 6 - 28001 Madrid.* ***Origin****: The data that we process comes from the organisation with which the controller has a contractual or service provision relation and to which end they must have the personal data of contact people for administrative and operational management in order to manage their access, addition to the intended project/service and/or verification of compliance with regulations under the responsibility of the organisation (e.g. data on*

*workers who are going to perform the contracted jobs in terms of coordination of company activities and prevention of occupational hazards). The **data structure** that we process does not contain sensitive data, except in those cases where the owner is beneficiary of special conditions or has to provide records that prove or justify compliance with said condition. Our Privacy Policy can be found on the corporate website"*

ADDITIONAL INFORMATION DATA PROCESSING OF VIDEO SURVEILLANCE AND ACCESS RECORDS:

What is the purpose of processing the personal data that you provide to us? (*) The list of RAFIA INDUSTRIAL S.A.'s activities is available at www.rafiaindustrial.com
• Access/visits control and video surveillance of the facilities, as well as safety and regulation compliance in them, to keep the people, goods and installations safe, as well as to perform duties to monitor workers as established in article 20.3 of the Workers' Statute, investigation of possible incidents or accidents, manage associated insurance and manage warnings or penalties due to breaches of safety regulations, via the video surveillance system.
• Verify that employees are fulfilling their job obligations and duties in accordance with article 20.3 of the Workers' Statute, which allows the employer to use surveillance and monitoring methods to this purpose (monitoring regarding the use of the images captured by the video surveillance systems to investigate accidents and/or incidents that may occur, as well as breaches of labour regulations, crimes or illegal conducts).
• Health and safety management (occupational hazard prevention and safety monitoring) and evaluation of compliance
• Monitoring of working hours and/or presence or attendance and of performance
• Management of Regulation Compliance (applicable regulations as well as mandatory internal regulations): Investigation, monitoring and audit of controls established to prevent crime with the possibility of establishing controls at the facilities access, information and document printing systems for all personal data that is under the responsibility of the organisation and therefore for all of the company's information systems, as well as controls pertaining to the use of the images recorded by the video surveillance systems to investigate accidents and/or incidents that may happen, as well as breaches of labour regulations, crimes or illegal conducts.
• Management of Accesses/Visits and Video Surveillance of the Facilities, as well as of safety and compliance with regulations in them, investigation of possible incidents or accidents, management of associated insurance and of warnings or penalties due to breach of safety regulations.
• Others (specify): investigation of possible workplace incidents or accidents, management of associated insurance, as well as investigation of incidents and confirmation of compliance with safety and personal data protection regulations established in the data protection systems and management systems for all personal data that is under the responsibility of the organisation and therefore for all of the company's information systems, as well as controls pertaining to the use of the images recorded by the video surveillance systems to investigate accidents and/or incidents that may happen, as well as breaches of labour regulations, crimes or illegal conducts.
• Time-based body temperature monitoring in order to access the facilities, with the following purpose (to detect potentially infected people and to prevent their access to a certain place and their contact with other people inside it): - To protect the health and life of the people who are at this workplace. - To contribute to containing the pandemic. - To comply with occupational hazard prevention regulations. - To verify that the workers meet the obligation to come to the workplace without fever.
• Inclusion in the reporting channel systems of the data associated to the disclosure (including anonymously) of the perpetration, within the organisation or within the actions of third-parties contracting with it, of actions or conducts that may be contrary to applicable general or industry regulations.
How long do we keep the data provided?
• The images/sounds recorded by the video surveillance systems will be eliminated within a maximum period of one month from their recording, except if they have to be kept to prove the perpetration of acts that threaten the integrity of people, assets or facilities (in which case the images will be made available to the competent authorities within a maximum period of 72 hours from when the existence of the recording was known), or if they are related to serious or very serious criminal or administrative offences regarding public safety, with an ongoing police investigation or with ongoing legal or administrative proceedings (Instruction 1/2006 of 8 November, of the AEPD, on personal data processing to purposes of surveillance via camera or video camera systems and Art. 22 OLDPGDR) – 30 days. • The data included in the automated files created to monitor access to buildings (Instruction 1/1996, of 1 March, of the AEPD, on automated files established with the purpose to monitor access to buildings) - 30 days. • The data of the person communicating a complaint and of the employees and third-parties are kept in the complaints system to decide on whether an investigation should be proceeded with on the reported facts, as well as subsequently as evidence of the operation of the model to prevent crime by the entity, according to article 24 of the OLDPGDR. • The organisation has established as conservation period of the temperature monitoring data the time necessary to face potential legal action derived from the decision to deny access.
What is the legal basis for processing your data?
• The legal basis for processing your data is to meet a legitimate interest of the Controller: • Safety and cases of legitimate interest where the controller may be the injured party and it were necessary to process and notify the data of the breaching party to third parties, to ensure observance of regulations and defence of the interest of the data controller, as well as cases of legitimate interest in specific processing as contemplated in the OLDPGDR: Article 19. Contact data and individual employer data processing; Article 22. Processing to purposes of video surveillance; Article 24 Internal complaint information systems). • Article 20.3 and 4 of Royal Legislative Decree 1/1995 of 24 March, approving the Consolidated Text of the Workers Statute Act (Estatuto de los Trabajadores, **ET**): The employer may take all the measures they deem best for surveillance and monitoring to verify that the worker fulfils their job obligations and duties, maintaining due consideration for human dignity and taking into account the actual capability of disabled workers, if any. • The employer may verify the worker's illness or accident condition that they allege to justify their missing work, by means of a doctor check-up. The worker's refusal to submit to this check-up may lead to suspension of the economic rights that the employer may be bound to pay under these situations. • (*) Ruling by the Constitutional Court 39/2016, of 3 March (Law 218/2016), reasoning that this authority to monitor is authorised by article 20.3 of the ET, which expressly authorises the employer to adopt surveillance and monitoring measures to verify that workers fulfil their job obligations. This general authority to monitor established by law allows employers to monitor workers' compliance with their professional duties, and the consent by these workers to this effect is implicit in the formalisation of the work contract. The legitimacy of this purpose is fulfilled with the existence of several signs posted throughout the organisation facilities that advise of the presence of cameras and recording of images and with clear information, if possible in writing, informing that they will be recorded, with the sole purpose to monitor fulfilment of job duties and that they may be penalised pursuant to the images recorded in the event of proven non-fulfilment. Likewise, STS 77/2017 of 31 January 2017. • AEPD guide to video surveillance: Article 20.3 of the Workers' Statute allows the employer to take all the measures they deem best for surveillance and monitoring to verify that the worker fulfils their job obligations and duties, maintaining due consideration for human dignity and taking into account the actual capability of disabled workers, if any. These measures may include, among others, the recording and/or processing of images without consent. However, these practises are fully subject to the Data Protection Act and to Instruction 1/2006 and they must meet specific requirements.

- Compliance with the legal obligation to guarantee the health and safety of employees is specified as the legal basis for the processing associated with temperature monitoring. This legal basis is contained in this case in the following regulations:
  - Workers' Statute.
  - Law 21/1995 on Prevention of Workplace Hazards.
  - Royal Decree 664/1997 on protection of employees from risks related to exposure to biological agents on the job*
  - Procedure for the occupational hazard prevention services against exposure to SARS-CoV-2
  - Good practises guidelines in the industrial sector regarding Covid-19 (National Institute for Health and Safety at the Workplace).
  - Guidelines adopted by the organisation's Occupational Hazard Prevention service by legal certification and delegation of preventive duties.

Who can your data be communicated to?

- Organisations or individuals directly hired by the Data Controller to provide services connected to the processing purposes (specify): Security company hired
- Insurance Companies (specify): In the event of an incident or accident they are provided to insurance companies to investigate the incident in order to establish the scope and coverage of the insurance premium subscribed by the data controller.
- Law Enforcement and Safety Agencies (specify): To the extent required, a proven right to access within the investigation of a breach of regulations.
- The owner of the establishment, due to legitimate interest in protecting the assets in their property
- Judges and Courts, as well as Law Enforcement and Safety Agencies: To the extent required, a proven right to access within the investigation of a breach of regulations.
- In the event of temperatures above the healthcare threshold, the person will be denied access and they will be referred to the primary care services (if they are external) or to the health surveillance service (if they are internal) so that, following protocol, they will undergo diagnostic testing and other communications established pursuant to the pandemic control protocol.
- Compliance Report Channel (Complaints on breach of the data protection regulations are sent to the "Chief Privacy Officer" at the Group's headquarters): Access to the data contained in these systems will be limited exclusively to those who, integrated or not within the organisation, perform internal monitoring and compliance duties, or to the data processors that are eventually appointed to this purpose. However, access by other people, or even communication to third parties, will be legal when it is necessary in order to take disciplinary action or to follow the legal proceedings that are necessary, when applicable.

Under what guarantee is your data communicated?

Data is communicated to third parties who prove that they have a Personal Data Protection System pursuant to current legislation.

What are the methods for placing a claim?

If you deem that the exercise of your rights was not fully satisfactory, you may submit a claim with the national supervisory authority by addressing the Spanish Data Protection Agency, C/Jorge Juan, 6 - 28001 Madrid.

What type of data do we process?

Identification and professional picture and data, as well as the reasons for the visit and/or person being visited, time of access and exit from the facilities.
Temperature control data may also be gathered, insofar as temporary temperature monitoring is performed in order to access the facilities to purpose of controlling to avoid pandemics, according to the COVID Data Processing Protocol that may be established in terms of guaranteeing the workplace safety of the people in the organisation.

How is your personal data safely stored?

RAFIA INDUSTRIAL S.A. takes all the necessary steps to keep your personal data private and secure and in any case, it will comply with the content of Law 5/2014, of 4 April, on Private Security and its enforcement provisions. Thus, it establishes and informs you of the following safety measures:

- DUTY OF DISCLOSURE: Information is provided on the existence of the cameras and recording of images, in order to comply with the duty of disclosure set forth in article 12 of the GDPR via an informative device in a sufficiently visible location, identifying the existence of the processing, the identity of the controller and the possibility of exercising the rights established in articles 15 to 22 of the GDPR. The informative device may also contain a connection code or an internet address for this information. In any case, RAFIA INDUSTRIAL S.A. has at the disposal of the affected parties the information referred to in the said regulations in this Privacy Policy, referenced on the device. If a flagrant perpetration of an illegal action is recorded, the duty of disclosure is understood to be met when there is at least the informative device regarding the video surveillance.
- LOCATION OF THE CAMERAS: RAFIA INDUSTRIAL S.A. will only record images of the public street insofar as it is essential to the preservation of security. In no case will ASPLA install sound recording or video surveillance systems in areas aimed for rest or relaxation of the staff or public employees, such as dressing rooms, bathrooms, canteens and similar facilities.
- SOUND RECORDING: RAFIA INDUSTRIAL S.A. will only record sounds when the risks to the security of the facilities, assets or people derived from the activity carried out at the workplace are relevant, and always observing the principle of proportionality, minimal intervention and guarantees.
- LOCATION OF SCREENS: The screens where the images from the cameras are viewed are located in a restricted-access area, so that they are not accessible to non-authorised third parties.
- PRESERVATION: The images/sounds recorded by the video surveillance systems will be eliminated within a maximum period of one month from their recording, except if they have to be kept to prove the perpetration of acts that threaten the integrity of people, assets or facilities (in which case the images will be made available to the competent authorities within a maximum period of 72 hours from when the existence of the recording was known), or if they are related to serious or very serious criminal or administrative offences regarding public safety, with an ongoing police investigation or with ongoing legal or administrative proceedings (Instruction 1/2006 of 8 November, of the AEPD, on personal data processing to purposes of surveillance via camera or video camera systems and Art. 22 OLDPGDR) – 30 days.
- WORK MONITORING: The processing is performed to exercise the duties to monitor the employees as established in article 20.3 of the Workers' Statute, within its legal framework and with the limits inherent to it. Insofar as the cameras may be used to monitor work in accordance with article 20.3 of the Workers' Statute, the workers and their representatives are informed on these monitoring measures implemented by the employer, expressly stating that the purpose of the images recorded by the cameras is to monitor work, as specified in the inclusion notification clause and in this privacy policy.
- RIGHT TO ACCESS THE IMAGES: In order to fulfil the stakeholders' right to access, a recent photograph and the National ID of the stakeholder will be requested, as well as details on the date and time on which the right to access is being exercised. The stakeholder will not be provided direct access to the images of the cameras that show images of third parties. To prevent third-party rights from being affected, in the event of a request for access, we will issue a certificate that will specify the data that was the object of processing, with the utmost precision possible and without affecting the rights of third parties. For example: "Your image was recorded on our systems on the ___ of the month of the year between _ o'clock and _ o'clock. Specifically, the system records your access and exit from the facilities."

RAFIA INDUSTRIAL S.A. has formalised agreements to guarantee that we process your personal data correctly and pursuant to current data protection regulations. These agreements contain the respective duties and responsibilities towards you, and they contemplate which entity is best positioned to fulfil your needs. These agreements do not affect your rights by virtue of the data protection law. Please contact us if you wish to obtain further information on these agreements.
The Data Controller takes all the steps required to keep your personal data private and safe. Only authorised RAFIA INDUSTRIAL S.A. staff, authorised staff of third parties directly hired by the Data Controller to perform services linked to the processing purposes, or authorised staff with companies that invoice under the commercial name of RAFIA INDUSTRIAL S.A. (that have the legal and contractual obligation to keep all of the information

safe) have access to your personal data. All of the RAFIA INDUSTRIAL S.A. staff who have access to your personal data is required to undertake to observe the Data Controller Privacy Policy and the data protection regulations, and all third-party employees who have access to your personal data must sign the confidentiality agreements under the terms established by current legislation. In addition, third-party companies who have access to your personal data are bound by contract to store your data safely. To ensure that your personal data is protected, RAFIA INDUSTRIAL S.A. has an IT safety environment and takes the necessary measures to prevent non-authorised access.

CHANGES TO THE PRIVACY POLICY

RAFIA INDUSTRIAL S.A. reserves the right to implement, at any time, any modifications, variations, eliminations or cancellations to the content and their presentation that it deems convenient, therefore we recommend that you check our privacy policy whenever you deem it pertinent. If you disagree with any of the changes, you may exercise your rights pursuant to the above-mentioned procedure by sending an email to gdpr@rafiaindustrial.com

In compliance with personal data protection regulations, we process the information that you provide to us (as well as the personal data of other people that you may provide to us) with the purposes specified in this privacy policy. You thus declare that you have been informed, consent to and have informed and have the consent of third parties on whom you provide us personal data, for said processing.

By accessing the facilities subject to video surveillance, you expressly consent to the data processing in accordance with the clause and additional information on data protection, as well as to informing and having the consent from third parties whose personal data you provide to us for processing of the access record.

Also, by accepting and/or validating the process you declare that you are over 14 years-old and you have legal capacity *** and expressly consent to the processing of the data pursuant to the content of the clause and additional information on data protection. If you checked the box for consent, the legal basis for these purposes is your consent, which you may withdraw at any time.
(***) In those cases where you represent a person under 14-years-old or a legally disabled person, you declare under your responsibility that you have the guardianship or custody of the minor or the corresponding legal representation, and proof of this may be required by the Data Controller in order to authorise the accepted consent.