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), 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 and submit for your acceptance the following privacy policy:

Client:

Who is responsible for processing your data?	
Identity:	REYDE, S.A.
Postal address:	Pol. Ind. Mas Mateu C/ De l´Om, 15 - 08820 El Prat de Llobregat (Barcelona)
Telephone:	+34 934787600
Email:	gdpr@reyde.com
Why do we process your personal data?	
• 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".	
• 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 your 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.	
• Others (specify): In the event of deposit contracts, the Organisation reserves the right to carry out regular audits at client and other debtor facilities.	
How long do we keep your information?	
• Your information will be kept in our files as long as the commercial collaboration 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 by the stakeholder or by the Organisation. In any case, when the relationship is finalised, the data of the stakeholder will be duly blocked, pursuant to current data protection regulations. • The information will be kept in our files as long as the commercial relationship continues, based on the conservation timeframes established by current regulations (six years for accounting and tax information), 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). In any case, when the relationship is finalised, the information 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 software 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) – 4 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. • The pictures/sounds recorded by the video surveillance systems will be cancelled within a maximum period of one month from their recording, unless they pertain to serious or very serious criminal or administrative offences, with an ongoing police investigation or legal or administrative proceedings (Instruction 1/2006, of 8 November, of the AEPD, on personal data processing to purposes of surveillance with camera or video camera systems) – 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.	
What is the legal basis for processing your data?	

- The legal basis for processing your data is the performance of the commercial contract/order that regulates the provision of services by the controller, therefore the information requested is necessary for proper service rendering.
- The administrative, tax and accounting processing of your data complies with tax, financial and corporate regulations governing the data controller, therefore the information requested is necessary for compliance with regulations by both parties.
- Data processing as part of a commercial relation and/or contract, necessary to maintain it or to comply with tax, labour, financial or corporate regulations governing the data controller, data transfer within corporate groups to internal administrative purposes, for direct marketing, fraud prevention, as well as processing of the contact information and cases of legitimate interest where the controller may be the harmed party and it were necessary to process and notify the data of the breaching party to third parties in order to manage regulation compliance and defence of the interests of the controller and purposes of video surveillance as legitimate interest of the company to protect its assets.
- Your unequivocal consent by accepting the consent clauses set forth in the basic document regulating the commercial relation depending on the commercial channel for contact.

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): 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 Report Channel (Complaints on breach of the data protection regulations are sent to the "Chief Privacy Officer").
- Others (specify): Media and specialised journals to promote the organisation's activities. Likewise, if any communication is received via the website from a potential client located in non-EU countries, the express consent of the interested party is requested through the consultation form on the corporate website, by accepting the privacy policy that indicates possible communication of data to the company of the group whose scope of operation includes the country of origin: countries where there is a Commercial Agent or Agency.

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 your rights?

- "Any person is entitled to obtain confirmation on whether we are processing personal data concerning them, or not."
- "Interested parties are entitled 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 to the purposes it was collected for."
- Under certain circumstances, the interested parties may request limitation of the processing of their data, in which case we will only keep it to initiate or defend claims".
- Under certain circumstances and due to reasons pertaining to their particular situation, interested parties 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".
- 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 them to another data processor".
- 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@reyde.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 interested party and photocopy of the ID of the interested party and/or of the person representing them, as well as the document proving said representation. *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 the data processor 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 interested party.
General Procedure to Exercise your rights:	"Once the required information is received, we will respond to your request pursuant to REYDE's general procedure for exercising rights: *The data controller will provide the interested party with information pertaining to their actions based on a request pursuant to articles 15 to 22 (Rights of the interested party) 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 processor shall inform the interested party of any of these extensions within one month from receipt of the request, stating the reasons for the delay. *When the interested party submits the request by electronic means, the information will be provided by electronic means when possible, unless the interested party asks that it be provided in another way. *If the data processor does not process the interested party'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. *The data controller may refuse to act on the requests; however, they bear the burden of proving the manifestly unfounded or excessive nature of the request.

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.aepd.es).

How did we obtain your data?

- The interested party or their legal representative.
- Private organisation (specify): 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?
REYDE takes all the steps required to keep your personal data private and safe. Only persons authorised by the organisation, authorised third-party employees (who have the legal and contractual obligation to store all the information safely) have access to your personal data. All of the organisation's staff who have access to your personal data is required to undertake to observe the REYDE 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, the organisation has an IT safety environment and takes the necessary measures to prevent non-authorised access.
CHANGES TO THE PRIVACY POLICY
REYDE may modify this Privacy Policy, and if it makes any important changes, we will notify you through our Services, or by other means, to provide you with the chance to review the changes before they come into effect. 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@reyde.com. You state that the continuous use of our Services after publishing or sending a notification regarding our changes to this Privacy Policy means that the collection, use and shared use of your personal data are subject to the updated Privacy Policy.

Service provider:

Who is responsible for processing your data?	
Identity:	REYDE, S.A.
Postal address:	Pol. Ind. Mas Mateu C/ De l´Om, 15 - 08820 El Prat de Llobregat (Barcelona)
Telephone:	+34 934787600
Email:	gdpr@reyde.com
Why do we process your personal data?	
• 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.	
• 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.	
• Others (specify): The Organisation reserves the right to carry out regular audits at client and creditor facilities.	
How long do we keep your data?	
• Your information will be kept in our files as long as the commercial collaboration continues, and for the conservation timeframes established by current regulations, as well as the timeframes legally or contractually established for the implementation or prescription of any action by the stakeholder or by the Organisation. • The data will be kept in our files as long as the commercial relationship continues, based on the conservation timeframes established by current regulations (six years for accounting and tax information), 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). 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) – 4 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.
- Labour documentation or documentation pertaining to Social Security: Documentation or the computer records or media where the data was transferred proving compliance with obligations regarding membership, signing up, signing off or variations that, where applicable, took place regarding these matters, as well as documents proving payment and receipts proving payment of salaries and delegated payment of benefits (Article 21 of the Legislative Royal Decree 5/2000, of 4 August, approving the consolidated text of the Law on Offences and Penalties on Social Affairs) – 4 years.
- The pictures/ sounds recorded by the video surveillance systems will be cancelled within a maximum period of one month from their recording, unless they pertain to serious or very serious criminal or administrative offences regarding public safety, with an ongoing police investigation or legal or administrative proceedings (Instruction 1/2006, of 8 November, of the AEPD, on personal data processing to purposes of surveillance with camera or video camera systems) – 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.

What is the legal basis for processing your data?

- The legal basis for processing your data is the performance of the commercial contract /order that regulates the provision of services by the supplier and/or creditor to the controller, therefore the information requested is necessary for proper service rendering.
- The administrative, tax and accounting processing of your data complies with tax, financial and corporate regulations governing the data controller, therefore the information requested is necessary for compliance with regulations by both parties.
- Your data is processed as part of a commercial contract (Compliance with a proposal and/or contract by the supplier/collaborator) that is necessary to maintain it or to comply with it, to comply with tax, labour, financial or corporate regulations governing the organisation, as well as to meet the legitimate interest of data transfer within corporate groups to internal administrative purposes, for direct marketing, fraud prevention, as well as processing of the contact information and cases of legitimate interest where the controller may be the harmed party and it were necessary to process and notify the data of the breaching party to third parties in order to manage regulation compliance and defence of the interests of the controller and purposes of video surveillance as legitimate interest of the company to protect its assets.
- Your unequivocal consent by accepting the consent clauses set forth in the basic document regulating the commercial relation depending on the commercial channel for contact.

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): 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 (specify): AEAT (Spanish Tax Agency).
- Financial organisations (specify): Transfer and/ or management of payment instruments.
- Labour Unions, Staff Meetings/Workers' Committee (specify): 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 Report Channel (Complaints on breach of the data protection regulations are sent to the "Chief Privacy Officer").
- 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' Bylaws 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.
- Others (specify): Collaborators or Promoters of Events, Projects and Grants where the organisation participates for their technical or economic justification, Media for the Promotion of 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.

What are your rights?

- "Any person is entitled to obtain confirmation on whether we are processing personal data concerning them, or not."
- "Interested parties are entitled 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 to the purposes it was collected for."
- Under certain circumstances, the interested parties may request limitation of the processing of their data, in which case we will only keep it to initiate or defend claims".
- Under certain circumstances and due to reasons pertaining to their particular situation, interested parties 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."
- 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 them 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@reyde.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 interested party and photocopy of the ID of the interested party and/or of the person representing them, as well as the document proving said representation. *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 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 interested party.
General Procedure to Exercise your rights:	"Once the required information is received, we will respond to your request pursuant to the general procedure of REYDE for exercising rights:

	*The data controller will provide the interested party with information pertaining to their actions based on a request pursuant to articles 15 to 22 (Rights of the interested party) 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 interested party of any of these extensions within one month from receipt of the request, stating the reasons for the delay. *When the interested party submits the request by electronic means, the information will be provided by electronic means when possible, unless the interested party asks that it be provided in another way. *If the data controller does not process the interested party'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. *The data controller may refuse to act on the requests; however, they bear the burden of proving the manifestly unfounded or excessive nature of the request.
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.aepd.es).	
How did we obtain your data?	
• The interested party 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 works 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 works 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 works 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 works 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 (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?	
REYDE takes all the steps required to keep your personal data private and safe. Only persons authorised by REYDE, 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 REYDE staff who have access to your personal data is required to undertake to observe the REYDE 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, REYDE has an IT safety environment and takes the necessary measures to prevent non-authorised access. REYDE have formalised agreements to guarantee that we process your personal data correctly and pursuant to 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 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.	
CHANGES TO THE PRIVACY POLICY	
REYDE may modify this Privacy Policy, and if it makes any important changes, we will notify you through our Services, or by other means, to provide you with the chance to review the changes before they come into effect. 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@reyde.com. You state that the continuous use of our Services after publishing or sending a notification regarding our changes to this Privacy Policy means that the collection, use and shared use of your personal data are subject to the updated Privacy Policy.	

Video-surveillance:

Who is responsible for processing your data?	
Identity:	REYDE, S.A.
Postal address:	Pol. Ind. Mas Mateu C/ De l´Om, 15 - 08820 El Prat de Llobregat (Barcelona)
Telephone:	+34 934787600
Email:	gdpr@reyde.com
Why do we process your personal data?	
• Management of Accesses/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.	
• 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, 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.

How long do we keep your data?

- The pictures/ sounds recorded by the video surveillance systems will be cancelled within a maximum period of one month from their recording, unless they pertain to serious or very serious criminal or administrative offences regarding public safety, with an ongoing police investigation or legal or administrative proceedings (Instruction 1/2006, of 8 November, of the AEPD, on personal data processing to purposes of surveillance with camera or video camera systems) – 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.

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.
- Article 20.3 and 4 of Royal Legislative Decree 1/1995 of 24 March, approving the Consolidated Text of the Workers Bylaws Act (**"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' Bylaw 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.

Who can your data be communicated to?

- Organisations or individuals directly hired by the Data Processor 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.
- Compliance Report Channel (Complaints on breach of the data protection regulations are sent to the "Chief Privacy Officer").

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 your rights?

- Any person is entitled to obtain confirmation on whether we are processing personal data concerning them, or not, although the exercise of the right involves unique characteristics: An updated image is required to be submitted as complementary documentation, that will enable the controller to verify and prove the presence of the affected party in the records.
- The interested parties have the right to access their personal data, as well as, if applicable, to 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 and due to reasons pertaining to their particular situation, the interested parties 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 them 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@reyde.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 interested party and photocopy of the ID of the interested party and/or of the person representing them, as well as the document proving said representation. Likewise, in the case of video surveillance, an updated image that allows the data controller to verify and contrast the presence of the affected party in its records is required to be submitted as complementary documentation". *Address to purposes of notifications, date and signature of the requesting party (in the case of a letter) or full name and surnames (in the case of an email), or validation of the request in a private area of the communication channel with a personal code to authenticate their identity). *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 interested party.
General Procedure to Exercise your rights:	"Once the required information is received, we will respond to your request pursuant to the general procedure of REYDE for exercising rights: *The data controller will provide the interested party with information pertaining to their actions based on a request pursuant to articles 15 to 22 (Rights of the interested party) 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 interested party of any of these extensions within one month from receipt of the request, stating the reasons for the delay. *When the interested party submits the request by electronic means, the information will be provided by electronic means when possible, unless the interested party asks that it be provided in another way.

	*If the data controller does not process the interested party'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. *The data controller may refuse to act on the requests; however, they bear the burden of proving the manifestly unfounded or excessive nature of the request. In order to comply with current regulations regarding video surveillance, Instruction 1/2006 of the AEPD, we inform you that the recordings shall be kept for one month, 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 building".
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.aepd.es)	
How did we obtain your data?	
• The interested party or their legal representative.	
• Private organisation (specify): Security company hired to this purpose for the safety of the facilities.	
What type of data do we process?	
Image; Name, surnames, Tax ID, organisation that the person accessing the facilities belongs to, as well as the person in the organisation that they are coming to see.	
How is your personal data safely stored?	
REYDE takes all the steps required to keep your personal data private and safe. LOCATION OF THE CAMERAS: Images will not be recorded in areas to be used for workers' breaks. LOCATION OF SCREENS: The screens where the images from the cameras will be viewed shall be located in a restricted-access area, so that they are not accessible to non-authorised third parties. CONSERVATION OF IMAGES: The images will be stored for a maximum period of one month, except for the images that are provided to the courts and the law enforcement and security agencies. DUTY OF DISCLOSURE: Information will be provided on the existence of the cameras and recording of images by means of an informative sign showing a pictogram and text specifying the data controller where the interested parties may exercise their right to access. The pictogram itself may include the informative text. The Agency website contains models both of the pictogram and of the text, as stated in the notification of inclusion clause and in this privacy policy. WORK MONITORING: When the cameras are to be used to monitor work in accordance with article 20.3 of the Workers' Bylaws, the worker or their representatives will be informed on the 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 interested parties' right to access, a recent photograph and the National ID of the interested party will be requested, as well as details on the date and time on which the right to access is being exercised. The interested party will not be provided direct access to the images of the cameras that show images of third parties. If it were not possible for the interested party to view the images without showing images of third parties, a document will be provided to the interested party, confirming or denying the existence of images of the interested party.	
CHANGES TO THE PRIVACY POLICY	
REYDE may modify this Privacy Policy, and if it makes any important changes, we will notify you through our Services, or by other means, to provide you with the chance to review the changes before they come into effect. 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@reyde.com. You state that the continuous use of our Services after publishing or sending a notification regarding our changes to this Privacy Policy means that the collection, use and shared use of your personal data are subject to the updated Privacy Policy.	