CLEVR

BUILDING
SMART
SOLUTIONS

Privacy Policy for CLEVR Services

CLEVR NL B.V., a company registered in The Netherlands with registered number 33281311 whose registered office is at Hogeweg 226-D, 3815 LZ Amersfoort, the Netherlands, along with its subsidiaries, divisions, and affiliates ("CLEVR") develops and operates applications (the "Services ") that helps companies digitize and streamline core processes (the "Customer" or "You, Your"). CLEVR understands the importance of protecting and safeguarding Your privacy and the security of Your business data when You use Our Services.

When We refer to personal data in this Privacy Policy, we mean identifiable data relating to you ("**Personal Data**"). We process various Personal Data for different purposes, namely:

- **Your Personal Data**: We process Your Personal Data to enable Us to provide the Services.
- **Business Data:** We process Business Data if we have been instructed by You to process this Business Data on your behalf for the performance of the Services.

In this Privacy Policy, some definitions with an initial capital letter are used. The definition of these terms corresponds with the definition given in the GDPR ('Regulation (EU) 2016/679").

Applicability

This Privacy Policy forms part of the Service Order signed between You and CLEVR and describes Our privacy practices in general terms with respect to the following Services:

- CLEVR Solution:
  - PLM Retail
  - FSM
  - Promo Manager
  - Digital Desk
- Developer Tooling (i.e. ACR, APD)
- Business Tooling (i.e. Planboard, PDF Converter, Dashboard)
- Support services

This Privacy Policy tells You under which conditions We process Personal Data and what measures we have implemented to protect Personal Data. Please read it carefully and make sure that You fully understand and agree to it.

Note that this Privacy Policy does not cover:

- Our processing of personal data relating to individuals who interact with CLEVR's assets outside the Services (website visitors, our business prospects & contacts, etc.) with regards to which We act as data controllers. To learn more about Our privacy practices relating to those practices and individuals, please visit our [www.clevr.com/privacy].
- Products and online services from third parties incorporated in the Services with different privacy practices, which will be governed by their respective terms and conditions and policies.

CLEVR as Data Processor

You are the "Data Controller" of the Business Data we process while carrying out the above mentioned Services, and We are the "Data Processor" acting on behalf of You in accordance with Your instructions. In other words, the Business Data is provided to us in the framework of carrying out the Services and We are not responsible for Your privacy practices. The responsibility for establishing the appropriate legal basis and complying with any laws and regulations applicable to a Data Controller with respect to Business Data of Your employees and other Data Subjects, lies with You. You guarantee that the Personal Data data is not illegal and does not infringe the rights of third parties. You shall indemnify Us against claims by thirds parties, of whatever nature, in relation to the processing of the Personal Data.

We act as a Data Controller with respect to the processing of **Your Personal Data**.

Categories of Personal Data

We collect certain types of Personal Data when You sign up to Our Services, use Our Services and contact Our support team. Specifically, we collect the following categories of Personal Data:

Contact Data: When You sign up to the Services and create Your individual profile, You provide us with Your Personal Data. This may include your name, gender and position, contact details (such as e-mail, phone and address), account login details (e-mail address and passwords, as well as any other Your Personal Data necessary for the use of the Services.

Usage Data: When You interact with the Services, We may collect, record or generate certain statistical usaga data about Your use of the Services. Such usage data consists of connectivity, technical and aggregated usage Business Data. We collect this to improve the user experience, to identify performance issues or other service malfunctions.

Support Data: In the event You submit a support request We might need to collect the relevant support data to fulfill Your support request. For this purpose, We may access Business Data.

Communication Data: We log Your IP-address, unique device-ID and may assign other electronic identifiers in order to properly deliver the Services or for security purposes;

Payment Information. Your Personal Data about Your billing address and method of payment, such as bank details, credit, debit, or other payment card information.

Note: You are not required to provide Your Personal Data that we have requested. However, if You choose not to do so, in many cases we will not be able to provide You with Our Services or respond to requests You may have.

Data Uses

We process the Personal Data as necessary for the performance of the Services; to comply with Our legal and contractual obligations; and to support Our legitimate interests in maintaining, supporting and improving the Services. These include understanding how the Services are used, and how the Services are performing. This will create valuable insights which help us dedicate Our resources and efforts more efficiently, providing customer service and technical support; and protecting and securing the Services, Ourselves and the organizations and individuals we engage with.

Specifically, We process Personal Data, for the following purposes:

- To facilitate, operate, and provide the Services.
- To authenticate the identity of users and allow them to access and use the Services.
- To provide users with customer care, assistance and technical support services.
- To further develop, customize and improve the Services, and to improve the user experience.
- To support and enhance Our data security measures, including for the purposes of preventing and mitigating the risks of fraud, error or any illegal or prohibited activity.
- To comply with Our legal, regulatory, compliance and contractual obligations.

Data Location

Personal Data is processed by Us and Our authorized sub processors in different locations. We maintain offices in the Netherlands, Norway and Germany. Personal Data may be accessed from any of those locations (or other locations as reasonably necessary for the delivery of the Services) by Our employees personally tasked with providing the Services to You. Such access usually occurs in the course of providing You with customer support, technical assistance, etc.

The sub processors we use to process Business Data on behalf of You, are located in the EU,. A list of our current sub processors including the location where the Business Data is being processed can be seen here: https://www.clevr.com/terms-and-conditions. By signing up to the Services, You consent to your Business Data being transferred to the servers of our sub processors as set out in this Privacy Policy.

For Personal Data transfers from the EU to countries which are not considered to be offering an adequate level of data protection, we and our relevant sub processors have entered into Standard Contractual Clauses as approved by the European Commission.

Data Retention

Business Data will be retained and stored for the duration of the Services on behalf of Your organization and in accordance with Your instructions. After termination of the Services, the Business Data will be deleted and will no longer be accessible to You. Regarding Your Personal Data, We may retain some of Your Personal Data for as long as necessary for the purposes described in this Privacy Policy. This may include keeping Your Personal Data after you have deactivated Your account for the period of time needed for Us to pursue legitimate business interests, conduct audits, comply with (and demonstrate compliance with) legal obligations, resolve disputes and enforce the Service Order.

Data Sharing

We may share Personal Data under the following circumstances:

- to a third party, in order to investigate, prevent, or take action regarding illegal activities, suspected fraud, by lawful request of public authorities and national security or law enforcement requirements, situations involving potential threats to the physical safety of any person, violations of the Services, or as otherwise required by law. In such circumstances, You acknowledge We may disclose such information to the extent necessary to comply with such legal requirement;
- Disclosures to sub processors as listed in the FAQ list as presented at https://www.clevr.com/terms-and-conditions;
- Disclosures to Our service providers who perform services for us to assist us in the delivery, improvement and optimization of the Services. These service providers may have access to Personal Data, each depending on their specific roles and purposes, and are prohibited from using Personal Data for any other purpose than stated in the Service Order and We ensure that the service providers will maintain confidentiality regarding the Personal Data and will comply with the necessary instructions and security measures as determined in the Service Order and this Privacy Policy;
- In the event of any reorganization, merger, sale, joint venture, assignment, transfer or other disposition of all or any portion of our business, assets or stock (including in connection with any bankruptcy or similar proceedings) we may disclose Personal Data to a third party. In this event, We will use reasonable efforts to notify You before information about You is transferred and becomes subject to a different privacy policy.

Cookies

We use “cookies”, anonymous identifiers, pixels, container tags and other technologies in order for Us to provide the Services and ensure that it performs properly, to analyze Your activities, and to personalize Your experience. Such cookies and similar files or tags may also be temporarily placed on Your device. Certain cookies and other technologies serve to recall Your Personal Data, such as an IP address.

Data Security

In order to protect Personal Data held with us, We are using industry-standard physical, procedural and technical security measures, These measures shall include, but not be limited to:

- the prevention of unauthorized persons from gaining access to data processing systems (physical access control);
- the prevention of processing systems from being used without authorization (logical access control);
- ensuring that persons entitled to use a data processing system gain access only to such Personal Data as they are entitled to accessing in accordance with their access rights, and that, in the course of processing or use and after storage, Personal Data cannot be read, copied, modified or deleted without authorization (data access control);
- ensuring that Personal Data cannot be read, copied, modified or deleted without authorization during electronic transmission, transport or storage on storage media, and that the target entities for any transfer of Personal Data by means of Personal Data transmission facilities can be established and verified (data transfer control);
- ensuring that measures are implemented for subsequent checking whether Personal Data have been entered, changed or removed (deleted), and by whom (input control);
- ensuring that Personal Data Processed are processed solely in accordance with the Your instructions (control of instructions);
- ensuring that Personal Data are protected against accidental destruction or loss (availability control);
- ensuring that Personal Data collected for different purposes can be processed separately (separation control).

The internet is not in itself a secure environment and We cannot give an absolute assurance that Your Data will be secure at all times. Transferring Data over the internet is at your own risk and you should only enter Personal Data to and within the Services by using a secure environment. We strongly advise You to connect to the Services via secure and encrypted channels (https).

Data subject rights

We shall, to the extent legally permitted under the Applicable Law, notify You without undue delay when We receive a request from a Data Subject to exercise its Data Subject's rights (such as the right to access, rectification, erasure or restriction of processing).
Taking into account the nature of the processing and the information available to Us, (i) We shall assist You by appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of Your obligation to respond to requests for exercising the Data Subject's rights; (ii) at its own discretion, either (a) provide You with the ability to rectify or erase Personal Data via the functionalities of the Services, or (ii) rectify or erase Personal Data as instructed by You; and (iii) reasonably assist You to comply with its further obligations under the Applicable Law. The costs associated with such cooperation are not included in the agreed prices and fees and shall be borne in full by You.

Audits and Certifications

The Services undergo security assessments by internal personnel and third parties, which include infrastructure vulnerability assessments and application security assessments, on at least an annual basis. The following security- and privacy-related audits and certifications are applicable to the Services, as described below:

- ISO 27001/27017/27018 certification: We operate an information security management system (ISMS) for CLEVR NL B.V. and CLEVR DE in accordance with the ISO 27001 international standard and aligned to ISO 27017 and ISO 27018. CLEVR has achieved ISO 27001 certification for its ISMS from an independent third party.

Information about security and privacy-related audits and certifications received by our sub processor AWS, including information on ISO 27001 certification and Service Organization Control (SOC) reports, is available from the AWS Security Website and the AWS Compliance Website.

Changes

We may periodically update this Privacy Policy. We will notify you about significant changes in the way We treat Personal Data by sending a notice to the primary email address specified in the Service Order or by placing a prominent notice on our site https://www.clevr.com/terms-and-conditions.

Questions

Any questions about this Privacy Policy should be addressed to our security department by mail at: security@clevr.com

This Privacy Policy was last modified on the 1st of April, 2022.