GDPR – General Data Protection Regulation

Minimal personal information on the 'data subject' is collected and managed by our software products. Our company treats B to B information as personal information and protect this data with the highest possible integrity.

Applied Computer Technology, Inc. complies with the GDPR guidelines set forth on 25 May 2018 and has always considered safety and protection of customer's data as an integral part of best practices. This includes, but not limited to;

- Right of erasure
- Provision for request of deletion
- Back-up storage shelf life
- GDPR as a part of our SLA (Service Level Agreement)

Data Collection and Processing

ACT collects and processes personal data only to the extent our software has a basis for doing so. Most of the software's personal data collection is public in nature but treats all data with the upmost care. Registered users and guests of ACT's cloud-based tools provide such services pursuant to the Terms of Service and in accordance with the Privacy Policy and SLA. ACT obtains consent before collecting personal data and gives data subjects the opportunity to withdraw consent at any time or depending on when they delete their on-line persona.

Security Measures

ACT utilizes industry-leading technical and organizational security measures to secure personal data, including providing video call connections with encryption keys. We also provide account administrators multiple tools to ensure meetings are secure and access controls are appropriately configured. Any recorded customer content is stored with most respected data centers that have obtained the highest standards of independent third-party and privacy certifications, and account administrators retain control over such recorded content at all times. ACT also participates in annual independent third-party security assessments and penetration testing. For more information about ACT's security measures, please visit the Trust Center at the bottom of www.expocad.com.

Appropriate Agreements and Employee Training

ACT maintains appropriate legal agreements with third parties with whom it contracts to perform any data processing activities. In addition, relevant ACT employees are subject to a criminal background check and must complete annual privacy and information security training in order to reinforce policies and procedures relating to GDPR obligations.

Cross-Border Data Processing

ACT has filed for certification under the EU-US Privacy Shield and Swiss-US Privacy Shield Frameworks with the United States Department of Commerce. Such certifications provide a legal basis for cross-border data transfers from Europe to the United States under the GDPR, and evidence by ACT's commitment to Privacy Shield principles. For more information about the Privacy Shield program, please visit www.privacyshield.gov.

Designed Privacy

ACT conducts regular Data Privacy Impact Assessments when there is a material change in a service offering or business activity that impacts the collection or processing of personal data. The Data Privacy Officer evaluates these against industry-standard information security controls. If necessary, the data privacy officer applies a remediation schedule to address any gaps identified during the process.

Sensitive Personal Data

ACT, does not keep sensitive personal data such as genetic code or biometric data.

Personal Data

Our products do keep personal data. Meaning any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier. There is a wide range of personal identifiers to constitute personal data, including name, identification number, location data or online identifier. GDPR Personal Data applies to both automated personal data and to manual filing systems where personal data are accessible according to specific criteria. ACT's personal data that has been pseudonymised – eg key-coded and/or encrypted to protect identifiable information in the event of a breach. It is difficult to attribute the pseudonym to a particular individual. Our products are encrypted to 128 bit keys.

Data Subject

A data subject is any person whose personal data is being collected, held or processed. Any personal data can refer to anything from your name, home address.

Rules that are meant to help data subjects and enforce their rights against abusive personal data processing. In order for personal data to be processed, data subjects must give their consent for EXPOCAD® Web. The data subject must consent for 'Data Controller' and 'Data Processor' to collect and store data for data processing. As a data subject, you have the right to access data about you. This data can either be viewed on-line or reported. Automated decisions, or profiling are also restricted within the GDPR. As a result, a data subject has the right to not be evaluated on the basis of automated processing. Data subjects include the right to restrict processing, the right to data portability, the right to be forgotten, the right to rectification and more. To read more about these rights, check out www.eugdpr.org for EU citizens' rights.

Data Controller

Data controller means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data. EXPOCAD® users who are event organizers are Data Controllers. In the EU - where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.

Data Processor

EXPOCAD® is the data processor. It compiles, reports and identifies data for use with the EXPOCAD® family of products.

Breach

ACT will notify the Data Controller at most in 72 hours as per GDPR compliancy and without undue delay. In the event of a data breach, ACT will cooperate to investigate and remediate the breach, cooperate with any supervisory authorities and law enforcement, and assist with any notifications as required. Notification of a breach will be either directly through voice and/or email. Or, through the ACT Community Center. Ensure that you are a member of the Community by visiting www.EXPOCADcommunity.com and applying for membership. This is a closed user only community and you must be approved for usage.

Audits

ACT does internal audits on a regular basis by the data security officer to ensure compliance of the latest rules and regulations. External audits requested by Data Subjects or Data Controllers will not be honored, unless mandated by law or court of law. Our systems manage information for a significant number of customers. This data is of sensitive and timely in nature and would have the potential of exposure by a third-party auditor. Our strict data policy of no disclosure to any person or entity outside of the person or entity themselves would be considered a breach as well as a violation of ACT's privacy policies.

Remedies

ACT carries all relevant insurance and protection to cover loss. Specific GDPR coverage is being pursued. See our EULA (End User License Agreement) for extents of coverage and liabilities.

Applied Computer Technology, Inc. | EXPOCAD®
Corporate Headquarters: 69 S. LaSalle Street Aurora, IL 60505 USA
+1 630.896.2281 e-Mail Luv@expocad.com www.expocad.com