INSZoom + GDPR FAQ

May 18, 2018

Please describe the nature of services INSZoom provides.

INSZoom is a Software-as-a-Service (SaaS) provider, specifically immigration case-management software platform.

Is your organization a Data Processor or Data Controller?

We provide our customers GDPR support as a Data Processor. For entities outside the U.S., GDPR obligations apply to handling and processing of personal data when the entity is either targeting their services/product to EU member states or their activities involve monitoring behavior. Although INSZoom is not subject to GDPR and other EU Data regulations, our organization provides GDPR support and readiness for our customer's compliance requirements.

What types of 'personal data' categories (including sensitive information) do Controllers (aka Data Exporters) typically export in relation to your SaaS solution?

Under explicit consent from the controller and data subject, personal data has included: biographic information revealing racial or ethnic origin, legal information including criminal background if applicable, and other information related to global immigration, employment and relocation activities. Any and all personal data processed has been narrowly defined by the customer including non-public personal information. Our hosting, service and privacy agreements expressly stipulate the methods and means of our products security and technical organization. INSZoom.com, Inc. is a 'Privacy-by-Design' SaaS company.

As an INSZoom Customer or User – what are my responsibilities under GDPR if it applies?

The regulations define a “controller” or “data exporter” as the organization or entity that determines the purposes of the Processing of Personal Data. As an immigration, mobility and legal case management system, our customers are the “controllers” who collect the “personal data” of their EU data subjects or end-clients (e.g. business travelers, foreign national applicants, and sponsored employees). Their personal information is then collected and processed in our application for a case transaction agreed between the two parties. The customer retains ownership of and controls all personal and service data collected and processed on the application. Thus, they hold the primary responsibility for ensuring that the personal data and its use is compliant with EU data protection laws including GDPR.

Below are some key points to consider for GDPR compliance:

- Does GDPR apply: The GDPR may apply to organizations that are established in the EU as well as certain organizations established outside the EU but which are processing the personal data of EU citizens, depending on their activities.
- Rights of Data Subjects: Organizations should be cognizant of End-Users whose personal data they collect and use. The GDPR establishes enhanced rights for End-Users, and organizations should be able to accommodate those rights including clear consent, transparency on how their data is used, privacy and the End-Users retain rights to delete, move or change the data collected by the controller.
- Data Breach Notifications: Organizations that are controllers of personal data should have clear processes in place to comply with the GDPR requirement to report data breaches in accordance with the time frames set out within the GDPR.
- Data Processing Agreement: Where personal data is transferred outside the EU, a customer may need DPAs in place with its sub-processors to ensure an adequate level of protection for the transferred data.
- Data Protection Impact Assessment (“DPIA”): DPIAs usually describe organizations data processes and protective measures. This means periodic audits and clear internal policies on how personal data is handled.

Please describe the technology, operational and security measures in place to handle the processing of any personal data on behalf of the controller and data subject.

INSZoom.com, Inc. is a Privacy-by-Design company and possesses ISO/IEC 27001 certification. All data is formatted in an Encrypted SQL Database. Personal data processed under the ISO 27001 framework meets the following requirements:

- ISO 27001 mandates the listing of all relevant statutory, legislative, contractual, and regulatory requirements.
- Risk assessment requirements of the ISO 27001 mandates the implementation of a Data Protection Impact Assessment and undertaking an evaluation of privacy risks.
- Asset management requisites of the ISO 27001 include personal data as a valuable information security asset which must define which personal data are involved in your operations, its origins, where to store it, for how long, and who will have access to these including any applicable supplier and storage relationships.
- ISO 27001 dictates systems acquisitions, development, and maintenance, which requires data security as an integral component of information systems throughout its lifecycle.
- Breach notification strictures under the ISO 27001 entail an efficient and consistent method to deal with data security to notify authorities within 72 hours after the discovery of a personal data breach.
- ISO 27001 uses risk assessments to identify the necessary controls regarding risk management, data protection impact assessments, and mitigation to the risks regarding rights and freedoms of data subjects.

Is client scoped data transmitted, processed, stored, disclosed to or retained by third parties? If yes, explain and describe the technology, operational and security measures in place to handle the processing of any personal data on behalf of the controller and data subject.

Per existing hosting and service agreements, INSZoom utilizes Amazon Web Service (AWS) for its data storage needs. AWS has posted all its related data processing services and obligations online and in confirmed DPA and addendums. AWS has affirmed that they will maintain our customer needs regarding confidentiality, audit, security and privacy including but not limited to incident response, ongoing monitoring, data sharing and secure disposal of all

applicable categories of personal and private data. AWS further affirms that all processed data on behalf of our customers will be under defined parameters for access, use and disclosure.

AWS is already providing specific features and services which help customers to meet requirements of GDPR including:

- Access Control: Only authorized administrators, users and applications have access to AWS resources
- Monitoring and Logging: Overview and visibility on activities regarding AWS resources
- Encryption and Strong Compliance Framework and Security Standards

More info can be found here: https://aws.amazon.com/compliance/gdpr-center/

Please describe how else INSZoom will be able to meet their customer's GDPR readiness.

- No controller or data subject personal data is subject to cross border data flows outside the U.S. especially in the EU.
- All data is stored at our hosted servers with Amazon Web Services in North America (U.S. for our U.S. clients and Canada for Canadian clients).
- No controller or data subject personal data is shared with any unauthorized third party including contractors or outside entities such as credit, consumer or marketing entities.

Per our customer’s respective hosting and service agreements and within the defined scope of service, INSZoom affirms the following:

- INSZoom will process our customer’s data for the sole purpose of providing the services according to their instructions and hosting and service agreements
- INSZoom will implement and maintain technical and organizational measures to ensure a level of security appropriate to the risk as set out by the GDPR and related regulations
- INSZoom will inform our customers without undue delay of requests from their Data Subjects exercising their Data Subject rights addressed directly to INSZoom regarding our customer’s personal data

- INSZoom will maintain and commit themselves to our customer's confidentiality and not process such personal data for any other purposes, except on instructions or unless required by applicable law.
- INSZoom will make every good faith effort to assist and cooperate with our customer's reasonable requests for GDPR related assistance regarding Information, Audit, Return/Deletion, Processing, Assistance and Records requests.

Additional information about the GDPR is available on the official GDPR website of the EU.