iSensing GDPR

V2

Harvey Beilinsohn
ISENSING LTD Belfast, UK

Contents

GDPR

Principles

- Processed lawfully and transparently, interests, and accurately for no longer than required – Data is anonymised, aggregated and turned into analytics as soon as it is collected by hashing and collected for only the period the customer specifies for a project. This information is built into our workflows and automated process to ensure accuracy of requirements and privacy.
- Collected for legitimate – We only collect data as specified by iSensing customer requirements as set out in a tender or contract. This information is built into our workflows and automated process to ensure accuracy of requirements and privacy.
- Retained securely – Only aggregated analytics are retained and the underlying anonymised data is deleted.

Individuals rights

- to be informed – We have notification signs that can be deployed with or in advance of sensors being activated. We can also issue technical documents to support mail-shots to customer mailing lists.
- of access – We give customer access to analytics which can be shared by the customer to their end users if required.
- to rectification – Analytics can be deleted from our system at the customer's request and we have a defined data destruction policy
- to restrict processing – Automatic processing can be stopped at the customer request and we have a defined de-activation process within 24 hours. Manual filtering can also be defined.
- to erasure – We have a defined cease process to deal with requests within 24 hours

- to portability – Aggregated analytics is available through an API and dashboards for our customers and stored in the EU.

Accountability & Governance

- Technical Measures – Data is hashed for security and regular security audits are conducted on our servers.
- Organisational Measures – We have an access control list and process inside iSensing to provide internal security controls.

Transfers

- Outside of EU transfers – For EU customers we do not transfer data outside of the EU.

Breach

- Notification process – We have a notification process right up to CEO level to deal with any breaches within 72 hours.