ISONAS General Data Protection Regulation (GDPR) Policy

The end user is responsible for entering personal information into the ISONAS Pure Access Cloud portal. This data can include name, credential, phone number and / or email. Please see your company security administrator responsible for entering data into the ISONAS Pure Access Cloud system for exact details regarding custom fields that the security administrator may have created. ISONAS does not track nor have knowledge of custom personal information that the customer security administrator may have entered. The data is stored securely in the ISONAS Cloud platform and only stored for the explicit purpose of use within the ISONAS Pure Access Cloud application. No data is shared, processed or exposed with the exception of integrations that may require data for third party integrations, for example, badge printing or VMS integrations. This sharing of data is controlled solely by the customer's security administrator. Data is retained in backups for 12 months at which time it is purged from the system. Data access within ISONAS is restricted to ISONAS administrators that require access to maintain the system. ISONAS is not responsible for the on premise version (Pure Access Manager) as it is provided with no data and installed/configured on the customer's premises and under the customers control exclusively.

By inputting data into the ISONAS system the customer agrees that upon separation and / or deletion of data the following will be true:

1. ISONAS is allowed up to 30 days to permanently delete
2. The data will remain in near line backups (storage not related to the primary platform) for up to but not to exceed 48 hours where it is only accessible by ISONAS administrators
3. The data will remain in off line backups (storage not related to the primary platform) for up to but not to exceed 12 months where it is only accessible by ISONAS administrators

For further information, please feel free to contact our team at support@isonas.com.

4/26/18