Identify and manage GDPR risks and easily respond to Subject Access Requests

Discover, manage and process Personal and Sensitive Data and respond to GDPR Subject Access Requests (SARs) quickly, easily and accurately with our end-to-end SAR Workflow.

1. Discover

AI.DATALIFT is a cloud-based platform that creates and maintains a rich index of data against an organisation's existing systems.

It has a wide range of connectors that have minimal installation footprint and are deployed to gather both metadata and content for fast and efficient analysis in the Cloud. This supports detection of personal and sensitive data, with no impact to the original data, which remains in-situ.

AI.DATALIFT analyses content uploaded to the Cloud to enable fast keyword and phrase searching. For example, you can search for ex-employees, inactive customers or project information based on unique references.

In addition, detection of standard complex content patterns such as Credit Card, Bank Account and UK National Insurance numbers, and Personal Sensitive Data, including racial or ethnic origin, provides an accurate risk profile within data. Custom patterns can be created to identify and classify content containing patterns that are uniquely important to your organisation.

2. Classify

On a scheduled basis, **AI.DATALIFT** can analyse new and modified content to classify previously unidentified personal and sensitive information.

Using these Classifications, your business can easily determine if this content is stored appropriately and with relevant security policy, and where this is not the case, implement remedial action through an information governance Policy;

> Archive to Azure and defensibly delete from the existing system

> Immediately delete from the existing system

> Report to Business Owner for resolution

Archived content is subsequently managed by disposal policies, preventing over-retention. This gives organisations a recovery option for a limited time based on their own approach to risk management.

Identify and manage GDPR risks and easily respond to Subject Access Requests

3. Govern

To comply with GDPR, it is vital that your organisation clearly documents the personal and sensitive information that is being stored, its source, why it is being stored, how long it will be retained, who has access to it, any fully automated decisions that were based on this information, and any organisations with which you share the data.

Using out of the box functionality, it is possible to create any type of GDPR Classification required to cover any of the wide range personal and sensitive data stored by your organisation, and to document those mandatory GDPR-compliance fields. In addition, authorised users are alerted to configure and initiate the relevant automated dispose or archive information governance policy for each of those GDPR Classifications.

The powerful combination of configurable GDPR Classifications, information governance Policies, non-compliance alerts and a comprehensive, automated, tamper-proof audit trail ensures that your organisation's data is fully governed in compliance with the regulation, with governance managed in one central system.

4. Respond

When your business receives a Data Subject Access Request, using the powerful search capabilities of **AI.DATALIFT**, all documents identified as applicable to the Data Subject are available for a review within seconds.

An authorised user then reviews the documents and decides if any should not be disclosed to the Data Subject for reasons that are explicitly described in the GDPR regulation, for example it would disclose personal or sensitive information about another person. Copies of documents that are approved for release are then assembled into a bundle that can be securely transmitted to the Data Subject, complete with a full report of the documents discovered, reviewed and released. A full audit trail is maintained to demonstrate compliance, if required.

The real-time GDPR Response dashboard tracks the status of all Data Subject Requests, and measures response time against the one-month period mandated by GDPR. A similar workflow is available for Right to be Forgotten/Right to Erasure requests.

Need to manage your GDPR compliance?
For more information on our GDPR solution, visit
https://www.automated-intelligence.com/solutions/gdpr/