Xiaa Solutions

Responding to a SAR for Overworked DPO's

The General Data Protection Regulation (GDPR) relates to the storage and use of personal information by an organisation and sets out seven key principles:

- Lawfulness, fairness and transparency
- Purpose limitation
- Data minimisation
- Accuracy
- Storage limitation
- Integrity and confidentiality (security)
- Accountability

An organisation has to comply with these principles (also covered by ISO27001 under "Information Security Policies"). As is well reported in the media, there can be significant penalties for information breaches.

General responsibility for securing data management would usually fall to the Data Protection Officer (DPO) to ensure that:

- Data is stored in known, protected locations that is only accessible on a need to know basis.
- That there should be no "information leakage". For example, with home working becoming more common in "pandemic" times, Personal Identifiable Information (PII) should not be "leaking" onto user's home computers.
- When Subject Access Request's (SARs, or Data SARs) are received, where a person requests a report on the data held by them by the Organisation, then these should be responded to in a timely way. The GDPR specifies inside 30 days. Note that SARs can also be raised by (ex)employees – a trend that is presently increasing.

These three responsibilities can be onerous, time consuming, and expensive to complete unless a solution such as the eSpyder GDPR Compliance Platform is used.

eSpyder is a distributed search engine that searches for and indexes PII information across the servers, data stores, and end-user PC's in an Organisation. A central portal (on-prem or cloud) is used to define searches, and then these are distributed out to an agent on each endpoint (PC or Server). The agent runs searches on scheduled basis (e.g. daily) and reports back to the portal whether any such information is available on its storage. Note that the actual PII information is not returned to the portal as this would give rise to a data lake of PII information – not something that is desired.

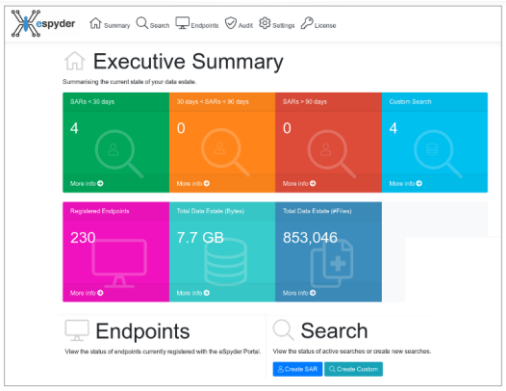
For Further Information:
Email: sales@xiaa.co.uk
Telephone +44 (0)208 412 7107

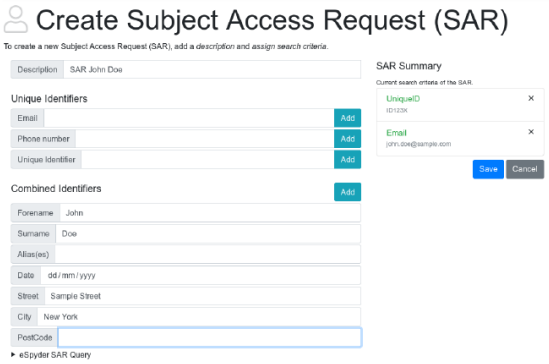
Xiaa Solutions

The user (the DPO or one of his team) see the results of the distributed search and can then either:

i) Take remedial action, because PII data has been found in a place its not meant to be, or

ii) Use the data location information to pull together a response to a SAR/DSAR. This can usually be done within 24 hours of the search, assuming that the agents are scheduled to run searches on a daily basis.





Importantly, eSpyder searches the content of files and databases to look for PII data. Many formats are supported, including Microsoft Office documents, PDFs, etc.

When a search is defined, it is normally best to use some unique identifier for the person (such as email address, account number, NI number, etc) rather than just the persons name. Searching for “John Smith” would return data on all documents that contained “John Smith” rather than for one unique individual.

Custom searches are also supported.

The benefits of eSpyder include:

- In the first instance, eSpyder maps out where PII data is generally stored, so that data can then be migrated to defined, secure, controlled locations.
- The migration can be monitored over time, and new leaks identified.
- SARs/DSARs can be responded to in a timely manner, which is often not the case if only manual processes exist.
- Responding to SARs/DSARs becomes a less onerous and less expensive task.

Please give us a call if you would like to know more.

For Further Information:

Email: sales@xiaa.co.uk

Telephone +44 (0)208 412 7107