

COPPEREYE SECURE DATA RETENTION SERVER - SDRS



THE CRITICAL IMPORTANCE OF COMMUNICATION RECORDS

Mobile telephony and the internet are now intrinsic parts of our everyday lives. Increasingly, the two technologies are combining driven by the convergence of the Notebook and the Smartphone. With every technological advance there are upsides and downsides. We can now communicate faster and more easily anywhere in the world, but we have now created an ideal environment for the criminals and terrorists of the world to operate every more remotely, secretly and swiftly. The evolution of Social Networking sites creates a new range of opportunities for people to roam with malicious intent. So how can the criminals and terrorists be tracked and monitored? Their activities, although invisible on the surface, create trail of their own which can be tracked, followed and investigated. Two main challenges exist and need to be fully addressed:

1. The criminals and terrorists are few in number and are hiding amongst hundreds of millions of other people in thousands and billions of communication interactions. How can you find what you really need and not get lost in the volume?
2. How do you ensure the data isn't abused and used for inappropriate and unapproved research?

According to the UK Home Office Website, there were 500,000 Disclosure Requests on Communications data in 2008. The data stores are becoming ever more critical.

LEGISLATIVE REQUIREMENTS

The governments of many states have legislated to ensure communications data is retained, and they are continuing to extend the legislation to address emerging technology, for example mobile Broadband. Although the legislation is different region by region (typically varying by items such as retention periods and customer SLAs), there are a number of common themes:

- **Secure retention** - of all communications usage data
- **Lawful compliance** - the data must be retained on a system that is only used for the purpose of law enforcement investigation.
- **Appropriate retrieval** - the ability to query data in a timely and proportionate manner and to retrieve only information that is specific to the security initiative being investigated.

- **Data Integrity** - ensuring the integrity of retained data is not compromised either through accidental or malicious activity.

- **Audit Trails** - ensuring querying of the retained data is by authorised personnel through secure and fully auditable means

- **Automatic Destruction** - guaranteeing that retained data and any disclosures generated are automatically destroyed at the end of the relevant retention period.

Legislation typically addresses the procedural elements of the data investigation and personal and data security. The technical challenges are left to the IT supplier to address.

COPPEREYE'S SOLUTION – SECURE DATA RETENTION SERVER

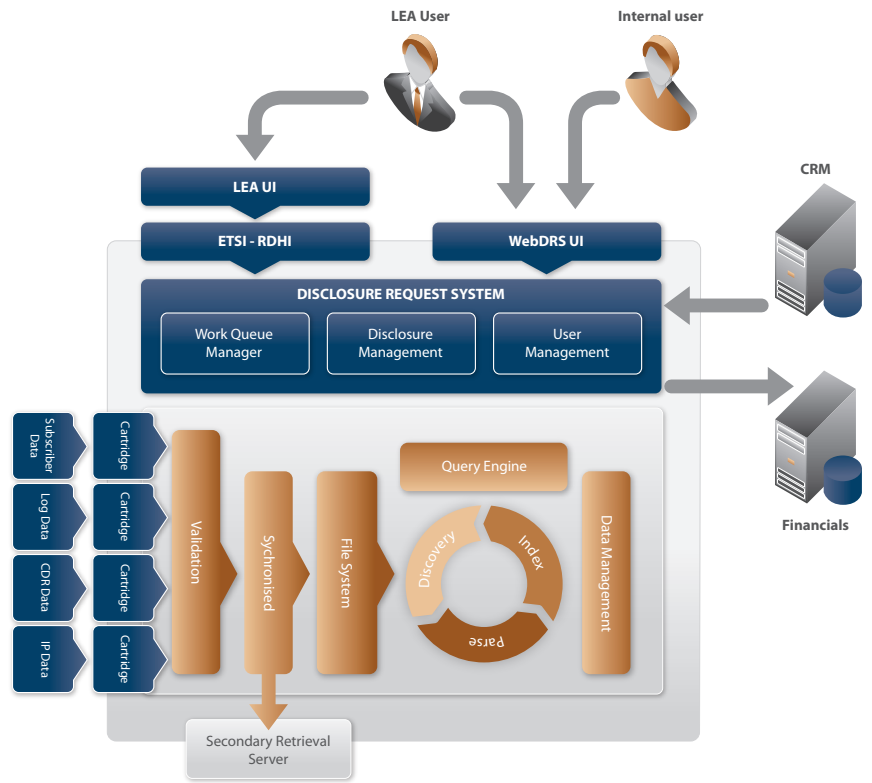
SDRS is CopperEye's full function solution to meet the demands of Communications Data Retention Legislation and Directives.

SDRS is built on CopperEye's Retention Server technology which addresses the technical challenges posed by the pure volume of records created. The core CopperEye technology thrives in environments of records in their billions. These technical capabilities are described in the CopperEye Retention Server Data Sheet.

CopperEye SDRS addresses all the legislative requirements that may be imposed on retention servers as represented by the diagram opposite.

SDRS applies to legislative need as follows:

- Secure retention** SDRS easily and economically supports increasing retention periods and extreme transaction volumes easily managing terabytes to petabytes of data. Specific data, should it be required, can also be encrypted as part of this process.
- Lawful compliance** SDRS is ETSI RDHI compliant. CopperEye is continually evolving its solution in support of the European Data Retention Directive (EU DRD).
- Appropriate retrieval** SDRS ensures that disclosure details are secured against inappropriate access and that any disclosed information is appropriate to the authority requesting a disclosure and will support queries on the most recent data with the fastest results of any solution on the market.
- Data Integrity** SDRS provides evidential quality retention. Communications records are retained with original content and format within their original files to guarantee the evidential quality of the data disclosed. All communication data files are stored in secure read-only, tamper-proof zones.
- Audit Trails** SDRS retains the full detail of all original communications records received from the network to ensure that any information required for disclosure is available as and when required.
- Automatic Destruction** SDRS can configure retention periods for data that is not only deleted, but shredded on a granular level.



In Summary, SDRS addresses the issues of Secure Data Retention in the following ways:

Issues	CopperEye SDRS Provisions
Meet EU and other legislative regulations and requirements	Meets all EU and other DRD regulations, first to market with ETSI interface
Simple and easy to install and operate	Simplest and quickest implementation of EU DRD
Easily expandable for new Reports created by users	Low cost entry through the use of new generation commodity hardware and operating systems
New data sources e.g. IP, email	Easily expandable for additional reporting (user report creation) and additional data feeds
Fully auditable	Transparent extension to access IP data
Secure and controlled access	All reports, access and history held for audit
Non-revenue generating project	Role based security and administration

UK Corporate Headquarters

CopperEye Labs Ltd, 1st Floor, 1 St Andrew's Hill, London, EC4V 5BY, UK
 t +44 (0) 1454 203 338 f +44 (0) 1454 203 330

e contact@coppereye.com
 w www.coppereye.com