

**Chairman:**  
Melanie Thatcher  
Baker Hughes Inteq  
Barclayhill Place  
Portlethen  
Aberdeen AB12 4PF

**Secretary:**  
Graham Payne  
Briar Technical Services Ltd  
501 North Deeside Road  
Cults  
Aberdeen AB15 9ES

---

### Position Statement Regarding Databases

With the impending implementation of the Harmonised Mandatory Control Scheme (HMCS), a number of Regulatory Authorities are discussing the possibility of data, supplied by vendors in Harmonised Offshore Chemical Notification Format (HOCNF), being held in a common database from which Hazard Quotients (HQ) may be calculated. Under such circumstances it is appropriate for EOSCA to reaffirm its policy regarding common databases.

EOSCA recognises the inherent data handling value of a common database but believes that access to the data should be **strictly controlled**. The various parties should have limited access only to data held in the database relevant to their own level of involvement, namely

Regulatory Authorities should have access to all data on HOCNFs **only** for products used within their **own** area of regulation.

Operators should have access to sufficient data (agreed minimum dataset) to allow them to calculate HQ **only** for products that they currently use within their **own** operations or products they are considering as substitutes for existing products being used or for new operations.

Vendors should be able to check data held **only** against their **own** products within the database.

No other parties eg Non Governmental Organisations NGOs, should have access to the data other than a simple listing of product names.

Data within the database remains the property of the supplying vendor. No data extracted from the database or values calculated from the data within it should be published in any form without the express permission of the supplying vendor.

The database should be managed under signed contracts between all parties concerned ie the Database Manager, the Regulatory Authorities, the Operator's Representatives and the Supplying Vendors. Access to data, as described above, should be strictly controlled by the Database Manager, with password and other protection as appropriate, especially if access is on-line.

November 2000