ABAC – Privacy Statement

Version 3.0 EN – 28/01/2016

Context

ABAC is the European Commission's corporate financial management system, used as well by other External Entities.
A description of the various modules and the supported functionalities can be found at https://myintracomm.ec.testa.eu/budgweb/en/abac/support/pages/its-020-020_intro.aspx

Access to ABAC is in general restricted to staff covered by the Staff Regulations and the conditions of employment applicable to other servants of the European Communities. Particular exceptions on this rule have been defined by DG Budget (Data Entry Agents, filing validation requests for legal entities and bank accounts). Furthermore, it is the responsibility of the Authorising Officer by (Sub-) Delegation (AOSD) to ensure that actors having direct or indirect access to the data and who are not subject to the Staff Regulations are legally bound to a non-disclosure agreement. For external contractors - such as IT-experts- this may take the form of particular provisions in the contract or the signing off of a separate non-disclosure agreement.

As ABAC collects personal data of individuals, the system is subject to the provisions laid down in the EC Regulation 45/2001 on the protection of personal data and the EC Accounting Officer holds the role of the Controller in that respect. The purpose of this privacy statement is to explain which data are collected for which purposes and how personal data is protected.

This privacy statement is applicable to all modules of the ABAC Architecture and can be changed by DG Budget without any prior notice.

Which data are collected?

ABAC only collects personal data on a "need to know" basis: any type of personal information that is irrelevant to operational financial management, ensuring the secured operation of the system and ultimately protecting the financial interests of the Communities is not maintained in the system.

For ABAC users

An ABAC user is anybody being granted access rights to one or multiple modules of the ABAC architecture.

An ABAC user is identified by a unique UserID. In exceptional cases, a physical person may have multiple UserIDs. The UserID uniquely identifies the physical person and is linked to the administrative data of this individual: name, office address and the organisation(s) to which the user is assigned. The UserID is the starting point for the management of the ABAC access rights and is used for logging the user's actions.

Any action performed under a UserID can be traced by ABAC in both visible and invisible records. In particular, any creation, modification and validation of a document will be logged and will be visible in the version management or the workflow records.

Invisible logging encompasses records being kept both within the ABAC system itself and at a technical level such as Databases or Operating Systems.

For referenced staff

Irrespective of whether a person has access to ABAC, other ABAC users can make a reference to him or her without the referenced person being notified of the registration. This referencing can be required by ABAC, notably to ensure that all the staff intervening in the validation process of a document is registered in ABAC or to assign a responsible person to a document. Furthermore, it is possible that the person is referenced in free text fields made available to the authorised users. As a consequence, ABAC can not in an exhaustive way define all positions where personal data is registered.

For third parties

Third party data subjects are to be understood as the persons having a legal or financial relationship with the management of the Community Funds. Third parties are recorded either as centrally validated legal entities or as (non-validated) mailing addresses assigned to Legal Entities. Note that any person working for the Community Institutions and bodies may also be recorded as a third party.

DG Budget, as the system owner, takes care of the notifications to the Data Protection Officer for all ABAC modules. However, it is the responsibility of the Authorising Officer by (Sub-) Delegation to ensure that the provisions related to the data protection are respected by his/her staff.

Why is the data collected?

First of all, the user data is collected to ensure that only duly authorised users are able to operate in ABAC according to the tasks and responsibilities officially delegated to them. Furthermore, the user's actions are traced to record the evolution of a file and to ensure that the AOSD has the complete image required before validating transactions in ABAC.

Any type of personal data can be used in the production of internal documents (e.g. the print out of a budgetary commitment), in reporting via the Data Warehouse and in production of official documents such as Debit/Credit Notes.

The information can also be used by any competent Auditing Instance such as the Court of Auditors, the Internal Audit Service and OLAF within the context of an audit.

How is the data protected?

As stated above, only the minimal set of personal data required for sound financial management is registered in ABAC. Access to ABAC requires an authentication based upon a UserID/password combination.

Visibility of data is protected by segregation: the user can only access information within the scope of each responsibility entrusted to him. Furthermore, particular provisions are implemented to manage access rights to personal data held in the legal entity and bank account file. The selection of the policy governing the protecting of personal data to be applied to ABAC for a given DG/Service, is the responsibility of the Authorising Officer by (Sub-) Delegation.

To whom is the information visible or accessible?

All information held within the legal entity and bank account file is shared and accessible to the ABAC user community and is visible to all staff being granted access to these data and to personal data held within certain groups of legal entities.

Where documents are produced by ABAC, user related personal data may be made visible to counterparties (e.g. contact persons).
Auditing instances may also access the personal data in the context of their respective audit missions.

Retention period

Taking into consideration the limited set of personal data registered in ABAC, the requirement to keep full records at least for five years after the discharge decision and the need to maintain information for audits, there is no "deletion" or "rendering invisible" of the personal data after a determined period.

Whom to contact in case of anomalies

Any modification to entries in the legal entity and bank account file are to be performed according to the standing procedures which require supporting documents to justify changes.

Any anomaly related to UserIDs and access rights should be first communicated to the responsible Local Profile Manager. He/she may wish to escalate the issue to the Master Profile Management team and/or the Local Informatics Security Officer in DG Budget.

In order to avoid anomalies on transactional level, the most important rule to respect is that no one shall use a UserID which is not assigned to him/her personally. In that regard, it is reminded that it is strictly forbidden to give one's UserID/password combination to colleagues and/or to use his/her credentials.

For any question related to your rights, you can contact the EC Accounting Officer, holder of the Controller function.

Any information relating to processing of your personal data is detailed in the register of the Data Protection Officer of the Commission:
http://ec.europa.eu/dataprotectionofficer/dpo_register_en.htm