moebius

How will you achieve 'Data protection by design and by default'?

This article gives an overview of the General Data Protection Requirement with regard to the use of software systems and describes how Moebius Business Software delivers data protection by design and default.

On May 25th, 2018 the European General Data Protection Regulation (GDPR) will become applicable harmonising the way in which personal data is managed throughout the European Union. The regulation is far reaching and, carrying a maximum fine of the greater of 4% of global turnover or €20 million, the penalties for non-compliance are potentially high.

The regulation affects a broad spectrum of businesses both inside and outside the EU which must now review and improve their data protection policies and procedures in order to be compliant.

This article considers the impact of GDPR on the way companies use and manage data through software systems and demonstrates how **Moebius Business Software meets the GDPR requirements for Data Protection by Design and Default** – as stated paragraph 2 of Article 25.

"The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons."[1]

This means that companies need data governance policies and procedures that ensure uniform management of data throughout their organisation, correct and appropriate access to data and that principles of data minimisation are all present by default in the systems used.

Control who can take what actions with what information

To ensure *'that by default personal data are not made accessible … to an indefinite number of natural persons'* companies need to have in place access controls to personal data that are applied from the moment of data capture.

Moebius is designed around security and the principle of protecting privacy of data.

[1] *Art. 25 GDPR Data protection by design and by default (https://gdpr-info.eu/art-25-gdpr/)*

Configurable security controls which users can perform specific processing actions on which data and can completely block access to specified data where required. For example, a defined group of users can be given access to add and edit personal data while another group may only view personal data and another may have no access at all.

Additionally, Moebius' system of inherited data security means that data can be easily partitioned so that **users perform processing actions on only a defined section of the data** according to the work that they are performing.

Personal data records are placed in groups and treated differently throughout the system with regard to access and processing. For example, the system applies different access rights to records recorded as suppliers or vendors to those recorded as customers.

Sensitive personal data such as religious beliefs or political opinions are easily identified and security features control access to this data meeting the GDPR's requirement to implement additional protection of data defined as "sensitive personal data".

Moebius uses pseudonyms to protect the identity of clients. The system presents links to the client using a pseudonym in place of the client name, allowing the identifying details of the person to be shielded from general access where required.

Once the **Moebius security model is designed it is applied by default** to new records. The system assigns access to new records by applying the pre-defined security model on saving of the record. This happens without user intervention and in a way that is opaque to the user.

Control reports allow designated personnel to view which users have access to personal data records and what type of access. This provides a full visual test of the data and functional security for all system users to ensure correct access.

Changes to access rights are propagated throughout the system such that if a Person's access is locked down, for example on ceasing to process the data (paragraph g of Article 28[2] *"…deletes existing copies unless Union or Member State law requires storage of the personal data")*, the **security changes apply automatically to all related data and documents.**

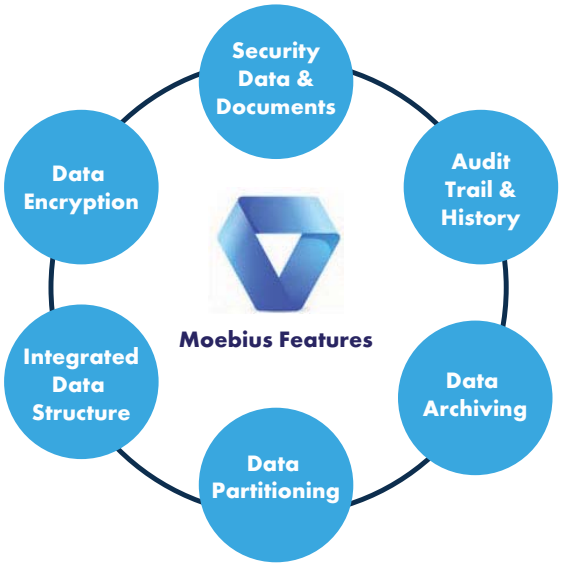
Documents are treated like data

Documents, such as passports, IDs and utility bills, contain details that are regarded as personal information and need to be managed with the same principles as the raw data.

The **GDPR ready features of Moebius that apply to data also apply to documents** uploaded to the integrated document management system.

In Moebius documents are related to their associated natural person and inherit the access rights from those entities such that a person's passport inherits the same security as the person. There are exceptions to this access which are managed within the context of use

[2] *Art. 28 https://gdpr-info.eu/art-28-gdpr/*



and/ or document type. For example, a user may have view rights to the person but be prevented from viewing KYC related documents. Or a Loan Agreement may be associated with a Money Transfer or Account Transaction as part of the transaction's supporting documents and can then be viewed by users with access the Money Transfer or Account Transaction.

These access rights are assigned as the documents are linked without user intervention.

As with data Documents can be partitioned using configurable security rules to **control which users can view, edit or delete documents**. In extreme cases documents can have unique security defined manually.

Present only data currently necessary - Data Minimisation

An important principal of the GDPR (Article 5) is that processing of Personal Data shall be limited to what is necessary.[3]

"The controller shall…implement appropriate technical and organisational measures…in an effective way…in order to meet the requirements of this Regulation and protect the rights of data subjects'. Article 23 calls for controllers to hold and process only the data absolutely necessary for the completion of its duties (data minimisation), as well as limiting the access to personal data to those needing to act out the processing"[4]

Data minimisation is an inherent feature of Moebius. For each area of the system where personal details may be used the natural person is selected by name and only the information relevant to the context of use is presented. And in addition only that to which the user has access. For example, a natural person linked to a company as a Director has only the Name and Address details revealed on the company director record. Only those users with permission will be able to access further personal information recorded about that natural person. At all times access to details such as Identification numbers or Date of Birth is limited to specified users that need to maintain and process that information.

Records that are no longer in active use are archived and removed from the general data view. Access to archived data is again controlled according to policies and procedures, and the implemented security module.

Data Portability

Under GDPR natural persons have the right upon request to receive a copy of their personal information in a *'commonly used and machine-readable format'*[5] and to request that the personal data be transferred without hindrance to another controller.

[3] *Article 5 GDPR states "adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation')" https://gdpr-info.eu/art-5-gdpr/*
[4] *GDPR Key Changes, https://www.eugdpr.org/key-changes.html*
[5] *Art. 20 GDPR Right to data portability https://gdpr-info.eu/art-20-gdpr/*

In Moebius users can **export to Excel, on demand, details of the Personal Data** of a natural person's record. Excel is a commonly used machine-readable format.

In addition, Moebius reporting suite can be used to create a structured report containing all the details related to a person's record and then generate the report to PDF.

The interconnected structure of the system means that it is easy to extract and report on all information related to a physical entity including any historical relations to other entities and records.

Integrity, Confidentiality and Accountability

Article 5 of the requirement sets out the responsibilities of data controllers and processors with regard to **ensuring data integrity and confidentiality**, and the need for controllers and processors to be accountable.

Moebius is a storage system for business information that centralises data from across many disciplines. Its system structure has clear separation of entities using relations to interconnect data where required. System functions include checks to prevent creation of duplicate records that present a challenge to efficient and correct management of personal data.

Regular data integrity checks and automatic DB fixes, with email notification of changes made to system administrators, help to ensure that the quality and integrity of data is maintained.

In addition to data checks Moebius has regular document scans to identify invalid or corrupted documents so that these can then be rectified in a timely manner.

Moebius is an **integrated system that records all details of the relationship with a person and therefore provides the 'journey' of the data from engagement/ letter of consent, to the end of relationship and eventual locking down of the data.**

Throughout this journey Moebius maintains a **full audit trail of all processing actions taken** on data and documents recording additions, changes and deletions identifying when the actions took place and which user performed the action.

This audit trail maintains records of any processing activities such as generation of Invoices, Money Transfers, Bank Accounts and Bank Account Transactions.

Companies wishing to achieve a higher level of protection of stored data can **opt to enable built-in encrypting back-up with no third party solution needed**.

What's next?

This article presents a limited review of the points of GDPR that relate to the storage and processing of data. The Requirement covers all aspects of protecting personal data from initial consent to deletion of data, covering topics such as securing network access and reporting of data breaches. To familiarise yourself with the full requirements they can be found in General Data Protection Regulation GDPR an easy to navigate document referenced throughout this paper.

The information provided in this paper should be regarded a guideline and not as legal advice.

Find out more about Moebius Business Systems on our web site or call 22 275 190.