Alemba Statement on GDPR

What is GDPR?

The General Data Protection Regulation (GDPR) is a new comprehensive data protection law in the European Union that updates existing laws to increase the protection awarded to personal data in light of rapid technological advances. Globalisation has increased the occurrence of complex international data transfers and usage.

GDPR replaces the patchwork of individual EU national data protection laws currently in place with a new single set of rules, directly enforceable across each of the 28 EU member states.

The GDPR regulates the "processing", which includes the collection, storage, transfer or use, of personal data about any EU individuals.

Any organisation that processes personal data of EU individuals, including tracking their online activities, is within the reach of this law, regardless of whether the organisation has a physical presence in the EU or not.

The GDPR's definition of "personal data" is very broad and covers any information relating to an identified or identifiable individual, often referred to as the "data subject".

The GDPR data protection rules provide more privacy rights to EU individuals and places significant obligations on organisations. The key changes are:

- Expanded rights for EU individuals: GDPR provides expanded rights for EU individuals such as deletion, restriction, and portability of personal data.
- Compliance obligations: GDPR requires organisations to implement appropriate policies and security protocols, conduct privacy impact assessments, keep detailed records on data activities and enter into written agreements with vendors.
- Data breach notification and security: GDPR requires organisations to report certain data breaches to data protection authorities, and under certain circumstances, to the affected data subjects. GDPR also places additional security requirements on organisations.
- New requirements for profiling and monitoring: GDPR places additional obligations on organisations engaged in profiling or monitoring behaviour of EU individuals.
- Binding Corporate Rules (BCRs): GDPR officially recognizes BCRs as a means for organisations to legalise transfers of personal data outside the EU where such transfer is required.
- Enforcement: Under GDPR, authorities can fine organisations up to the greater of €20 million or 4% of a company's annual global revenue, based on the seriousness of the breach and damages incurred.
- GDPR provides a central point of enforcement for organisations with operations in multiple EU member states by requiring companies to work with a lead supervisory authority for cross-border data protection issues.

alemba

Customer Data Held in the vFire Application

Alemba provides a number of tools and services to ensure vFire customers remain complaint with GDPR requirements.

Security and Data Restriction

Alemba would urge all customers to review their security roles within vFire, determining who has access to personal data. vFire provides the platform to record and manage who has access to what data, providing a mechanism to restrict data access.

Alemba would recommend that auditing is enabled for customer data fields so that all changes to these fields are recorded. This ensures that any customer requests for corrections to data being held are complied with.

An important feature of vFire is its ability to not only audit standard data fields, but also the administration settings of the system. This will ensure that no analyst has permissions they should not and that any unauthorised changes are recorded.

Location of Data Access

vFire provides the ability to restrict the ability of analysts and users to view data outside their region of authorisation. vFire's advanced field security rules are deployed to control this information.

If data is to be transferred out of the EU, the management and control process for that data can be automated using workflow templates, ensuring compliance with Binding Corporate Rules.

Data Deletion

Alemba provides data deletion and anonymisation tools for the vFire application. This allows any personally identifiable data to be anonymised and for data not to be retained for longer than necessary, allowing them to be forgotten. Alemba also provides a service to its customers to set up this function for them, if required.

Binding Corporate Rules

The powerful vFire request engine should be used to map your organisation's Binding Corporate Rules, allowing requests for changes to the storage, use of, addition to or deletion from to be recorded and properly authorised.

Management of Data Sources

vFire provides the platform to determine where data about customers is held, record and track changes to that structure.

Alemba can help you configure vFire process to on-board, change, regionally restrict and delete customer data throughout your organisation.

Data Use Breaches

vFire provides the ideal platform to automate you data breach procedure, allowing rule based analysis to determine severity and the corresponding corrective actions and notification rules to be actioned and enforced.

Alemba Statement on Internal Compliance with GDPR

Alemba has reviewed and updated all our internal processes, procedures, data systems and documentation to ensure that we are ready when GDPR comes into force in May 2018.

Alemba's GDPR Principles are:

- Data is processed fairly and lawfully
- Data is processed only for specified and lawful purposes
- Processed data is adequate, relevant and not excessive
- Processed data is accurate and, where necessary, kept up to date
- Data is not kept longer than necessary
- Data is processed in accordance with an individual's consent and rights
- Data is kept secure
- Data is not transferred to countries outside of the European Economic Area ('EEA') without adequate protection