GDPR and Aderant Expert

The EU General Data Protection Regulation is an update to the Data Protection Directive 95/46/EC, which goes into effect on 25 May 2018. The purpose of the GDPR is to protect EU citizens (data subjects) from privacy and data breaches. The regulation outlines the requirements for privacy and data protection for any organizations (data controller/data processor) that hold or process personal data of individuals residing in the EU, regardless of where the organization is located. More information on the GDPR can be found at www.eugdpr.org.

Below is a summary of the key components of the GDPR, as documented at www.eugdpr.org, and how it applies to the Aderant Expert product.

Breach Notification Summary

Under the GDPR, breach notification will become mandatory in all member states where a data breach is likely to "result in a risk for the rights and freedoms of individuals." This must be done within 72 hours of first having become aware of the breach. Data processors will also be required to notify their customers, the controllers, "without undue delay" after first becoming aware of a data breach.

Impact of Breach Notification to the Aderant Expert Product

None.

The responsibility of notifying affected data subjects of a breach of privacy and data resides with the organization who is utilizing the Aderant Expert product.

Right to Access Summary

Part of the expanded rights of data subjects outlined by the GDPR is the right for data subjects to obtain from the data controller confirmation as to whether or not personal data concerning them is being processed, where and for what purpose. The data subject may also request corrections to inaccurate

personal data, as well as to cease of further processing of personal data while still allowing the data to be stored in the controller's system. Further, the controller shall provide a copy of the personal data upon request, free of charge, in an electronic format.

Impact of Right to Access to the Aderant Expert Product

Low.

The Aderant Expert product provides a full suite of reports that may be used to deliver personal data that is stored within Expert, as well as the intended purpose and use of that data throughout the Expert system, to the data subjects. Also, Expert provides the means to modify, update and correct personal data of the data subject, as well as the ability to flag the data as inactive or unavailable for further processing either on a temporary or permanent basis.

Right to be Forgotten Summary

Also known as Data Erasure, the right to be forgotten entitles the data subject to have the data controller erase his/her personal data, cease further dissemination of the data, and potentially have third parties halt processing of the data. The conditions for erasure, as outlined in article 17, include the data no longer being relevant to original purposes for processing, or a data subjects withdrawing consent. It should also be noted that this right requires controllers to compare the subjects' rights to "the public interest in the availability of the data" when considering such requests.

Impact of Right to be Forgotten to the Aderant Expert Product

Medium.

Aderant Expert provides the means to remove personal information about data subjects from structured storage within the system without compromising the integrity of the underlying modules or their transactions.

Personal data is centralized in structured storage within the Aderant Expert product and is not duplicated within the various subsystems of transaction processing. Only internal ID values that are unique to the Expert product are utilized by subsystems for transactional processing. These ID values do not contain any identifying details of, or private information about, the data subject. Therefore,

personal data may be removed from the centralized and structured storage locations while still preserving the internal ID values and underlying transactions.

At present, removing personal data requires the controller to visit multiple application forms. The next major release of Aderant Expert, version 8.2, will provide a centralized location within the application where all personal information about a data subject may be removed from structured storage.

Note that within the Aderant Expert product, there are also non-structured storage fields such as description fields, narrative fields, and documents if the organization is utilizing the Expert Case Document Management component. Users can input free-form text into these components that may contain personally identifying information about data subjects. The Expert application provides the ability to search these fields through the existing DM search and Conflicts of Interest search functionality. These search capabilities may be leveraged to locate personally identifying information that might be stored in non-structured fields, and to access the data and make any required GDPR adjustments.

Data Portability Summary

GDPR introduces data portability - the right for a data subject to receive the personal data concerning them, which they have previously provided in a 'commonly used and machine-readable format' and have the right to transmit that data to another controller.

Impact of Data Portability to the Aderant Expert Product

Low.

The Aderant Expert product provides a full suite of reports that may be used to deliver personal data that is stored within Expert, as well as the intended purpose and use of that data throughout the Expert system, to the data subject. Reports within the Expert system can be printed in electronic format, delimited format or be exported into other products such as Microsoft Excel for further formatting.

The next major release of Aderant Expert, version 8.2, will provide a centralized location within the application where all personal information about a data subject that is contained, and structured storage can be viewed and exported.

Privacy by Design Summary

Privacy by design as a concept has existed for years now, but it is only just becoming part of a legal requirement with GDPR. At its core, privacy by design calls for the inclusion of data protection from the onset of the designing of systems, rather than an addition. More specifically - *'The controller shall...implement appropriate technical and organisational measures...in an effective way... 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 minimization), as well as limiting the access to personal data to those needing to act out the processing.

Impact of Privacy by Design to the Aderant Expert Product

Medium.

Aderant Expert has a robust security model that provides the ability to secure personal and private information about data subjects only to those who are authorized for access. In addition, all transactions related to the data subject are securable, although the transactions themselves do not contain personal or private data about the data subject.

Furthermore, all data that is transmitted by the Aderant Expert application, through standard use as the product communicates with the services and with the database, can be encrypted. Encryption at this level is an opt-in approach, where the organization that is deploying Expert must obtain a secure certificate to enable secure communications. The organization may also encrypt sensitive fields in the underlying database tables so that the data is only accessible through the application layer and by authorized access to the application.

Data Protection Officers Summary

Data Protection Officers (DPOs) must be appointed in the case of: (a) public authorities, (b) organizations that engage in large scale systematic monitoring, or (c) organizations that engage in large scale processing of sensitive personal data (Art. 37). If your organization doesn't fall into one of these categories, then you do not need to appoint a DPO.

Impact of Data Protection Officers to the Aderant Expert Product

None.

Governance within the data controller and by the data processor is a responsibility of the organization itself based on how the data subject's personal information will be used. The Aderant Expert product is not typically utilized by organizations that qualify for a DPO. Regardless, the reporting capabilities and functional design of Expert provide a level of transparency and facility for the DPO to operate, should one be required by an organization that utilizes Aderant Expert.

Common Questions Regarding GDPR and Aderant Expert

Below are some frequently asked questions regarding data privacy, data security and the Aderant Expert product.

Does Aderant take privacy into account when designing its software?

Yes. Aderant takes privacy of personal data very seriously and privacy is taken into account when designing all features and functions of the Expert application. For example, the Expert product has provided the means to secure private and confidential data at the row level, through a robust security design that is a native part of the application and that is honored by all application functions, since 1995.

How does Expert Row Level Security (RLS) work?

Once RLS is enabled for an entity (Client, Matter), deny security takes precedence for that entity. The user will only be allowed to view and consume the entity if they've been given explicit rights to do so. All searches, queries, etc. will only return results to allowed records. Denied records are implicitly filtered out of the search results that are available to the user. If the user explicitly types in a record to which they have been denied, nothing will be returned – the behavior is analogous to the record not existing at all. All related data that is attached to the secured entity record is also implicitly secured by the Expert security infrastructure.

When reporting financial and other figures, will Client and Matter records that are secured be contained in the results?

Values for secured Matters will be included in the overall totals to ensure the accuracy of the data. However details of the individually secured Matters will not be available unless the user has explicit access to view the Matter's details.

How can information be found if a Data Subject Access Request is received from an individual?

A Conflicts Search may be performed, and in the case of the Expert Case product, a DM search may be performed. Additionally, a Names search or other types of searches, such as Client, Matter, Personnel, Vendor, Bank, etc., may be performed from within the respective functional application area. With the Expert 8.2 release, there will be a centralized area within Entity Manager where all GDPR related searches may be performed against structured, personally identifying data.

How is data deleted from the system to comply with a right to be forgotten request?

By design, Expert does not utilize personally identifying information for links throughout the system. A unique, internal ID (called an UNO) is generated for all records within Expert, including entity records (Clients, Matters, etc.). This UNO value is utilized within all transactional references back to the entity. In addition, all structured details about the entity, including personally identifying information, are centrally stored. This design allows for the removal of any personally identifying details without compromising the integrity of existing transactions.

The Expert 8.2 release will provide the ability to remove personally identifying information about an entity from structured storage with a single click. In prior versions of Expert, the Client Maintenance, Personnel Maintenance, Vendor Maintenance and Names Maintenance modules may be used to remove personally identifying information from structured storage.

For non-structured storage such as documents, narrative fields and description fields that contain free-form text, a DM search and a Conflicts of Interest search may be used to identify personally identifying data. Because information in non-structured fields may not be uniquely identifying, these search results must be carefully analyzed to determine if action is necessary to satisfy the right to be forgotten request.

When a right to be forgotten request is processed in Expert, how is cached data on local devices updated?

Locally cached data on connected devices is synchronized periodically through a background process with the central Expert database. Data change in the central database, including the processing of a right to be forgotten request, will be reflected in local cache upon next synchronization.

For disconnected devices that maintain a local cache, the data will be synchronized with changes in the central Expert database upon next connection to the Expert services.

Is the data encrypted at rest?

With Expert 81SP1 and higher, it is possible to encrypt sensitive fields at the table level, such as fields that contain salary data, social security numbers and other personal ID values, etc. SQL Server 2016 is a requirement to enable this level of encryption.

Data that is cached on hand-held devices that utilize Expert mobile functionality is encrypted, by default, across all versions of the Expert product.

Data that is cached on local desktops and laptops to facilitate offline functionality of smart client applications is not encrypted by the Expert application itself; this by design. Best practice guidelines for encrypting localized data on desktops and laptops, including documents, e-mail stores, etc., is to utilize a disk level encryption service such as BitLocker. Aderant Expert supports all levels of encryption at the disk level that is also supported by the underlying operating system.

Is the data encrypted in transit?

It is possible to encrypt data between communication endpoints of the Expert application. This includes:

- All traffic between the Expert client and the Expert Services. The firm must obtain their SSL certificate to enable this encryption.
- This applies to the Services Framework applications, which communicate with the Expert client via HTTP (HTTPS when SSL is enabled).

- Communication traffic for the Expert Browser modules can be encrypted through the same means today, across all versions of Expert. This includes all of the public APIs.

The Expert classic client-server modules utilize TDS encryption, across all versions of Expert.

Communication traffic for Expert On-The-Go functionality can also be encrypted, across all versions of Expert, and typically is encrypted in all deployments as a best practice. Again, the firm must secure their SSL certificate and enable encryption when deploying the On-The-Go services.

All traffic between the Expert Services and the Expert database may also be encrypted. The Expert services and the Expert database are usually within a controlled, secured data center and do not typically require this level of communication encryption. However this level of communication encryption is also available (requires SQL Server 2012 R2 or higher) and can be enabled across all versions of Expert.

Is Aderant Expert tested against recognized standards for security and privacy?

Yes. Aderant utilizes a third party, Insomnia Security Specialists, to assist with independent security evaluation of the Expert product on a periodic basis. In addition, there is a security expert within the Expert product team and security fundamentals are part of our new starter training program. The OWASP top 10 list is used as a guideline to ensure that the most common security concerns are accommodated by the Expert product, where applicable.