SUBJECT: GDPR and PII Regulations and Protection
EMAIL: June 5, 2018

Hello All,

Over the last few weeks many of you have reached out to EWS Group asking about MoversSuite's General Data Protection Regulation (GDPR) readiness and, more generally, about security as it relates to you and your customer's Personally Identifiable Information (PII) data. While we have been digging into GDPR and still have more work to do, we wanted to take a moment to give you an update on where we are at in the process and to offer you some suggestions.

We will discuss the following topics in this email:

- Encryption at Rest
- Encryption in Transit
- Customer Request of Data Removal
- Customer Request to View/Edit Personnel Information
- Other Related Items

IMPORTANT: Please note that we are not experts regarding GDPR and any information shared in this email regarding the GDPR is based on our research and our opinions formed by that research. Each company should do their own research, employ experts and attorneys where needed, so that you can better understand your legal GDPR and PII obligations as it applies specifically to you.

Encryption at Rest

Encryption at Rest specifically addresses the idea of your data being encrypted at the database level.

We know that some of you have already addressed this issue on your own to meet requirements of certain customers. There are multiple ways to accomplish encryption at the database level. You can do it directly in MS-SQL. Unfortunately, this currently requires an Enterprise version of MS-SQL, which can be expensive. Another option can be to use a third-party solution, such as NetLib Security's Encryptionizer for SQL Server. MoversSuite customers have used both MS-SQL and NetLib and have had successful results.

At this point, we recommend database encryption for all MoversSuite customers. We understand that for some of you, your van line will be requiring it in the future, as well.

For customers currently hosted in our **standard** Azure hosted environment, we are currently learning what it will take to encrypt your databases and will communicate with you directly once the plan to proceed is complete. For those using our Azure environment in a **non-standard** configuration, we will contact you once we have more details on the process and costs related to encryption.

For all other customers, we leave data encryption up to you and your IT resources. We will be glad to offer guidance regarding possible solutions, but ultimately each of you have different configurations and needs that may require unique solutions.

Encryption in Transit

Encryption in Transit specifically addresses the idea of your data being encrypted as it moves between the database and the applications that use the data. Below we address areas specific to EWS Group and our MoversSuite products:

> **MoversSuite Application** - Our application talks directly to the database via direct SQL access. In this case there is no encryption in transit. If MoversSuite is being used as intended, then the application exists within the same closed network as the database and there is a lower risk of security issues arising.
>
> **MoversConnect** - Our in-the-cloud API service (which hosts various interfaces) is acting as an intermediary between our customer's database(s) and the outside world. This service already uses a mix of proprietary encryption between MoversConnect and API services running locally for each customer. Further, SSL is utilized in communication through the internet. Additionally, the communication between MoversConnect and customer's databases via the APIs is set up for port to port communication. Therefore, MoversConnect is the only service that can communicate via the connection.
>
> **MSCrew** - MSCrew works exclusively through MoversConnect.
>
> **Van Line Interfaces** (not through MoversConnect) - A few interfaces currently exist with van line systems that do not communicate via MoversConnect. Each of these interfaces are governed security-wise by the van line, via security certificates using MQSeries, custom receiver applications, and SSL certificates for web service-based connections.

Customer Request of Data Removal

Customer Request of Data Removal is a provision of GDPR that allows a customer to request that their PII data be purged from your system. While thinking about this in general terms of a move that involves the van line and multiple agents who may be using different systems, it gets a bit convoluted. The GDPR references the various relationships between the data subject, the controller of the data, regulators, processors and sub-processors, and a need for a contract between each to guarantee data removal across systems once it is requested. GDPR does include exemptions in cases where removing data is not possible for accounting reasons and in cases where other regulations require the data be kept. GDPR also specifies a 30-day period in which you need to respond to the data removal request and remove the data from your systems, assuming no exemption exists.

From a MoversSuite perspective, we have concluded that we need to provide you with an admin related tool to remove PII information from an order. The tool, once available, will be accessible through our Admin Tool and will perform the following on a specified order:

- Replace the Shipper Name with the text "Data Removed"
- Remove the following:
    - Address Information, except for City and State

- Phone Numbers
- Email addresses
- SSN
- Credit Card Payment Information
- Other data identified as we dig into this process

Notes on Data Removal:

- The removal process will include removing the above data from all necessary tables in the MoversSuite database, which may include archived invoices, invoice header information, etc.

- Beyond archived invoices, we would leave the disposing of documents attached to the order to each customer, since we do not necessarily know which documents contain PII related data.

- If the same shipper has multiple orders, you will need to repeat the removal process for each order.

- We plan on having this tool available around the end of the 2018 summer season.

Customer Request to View/Edit Personnel Information

Customer Request to View/Edit PII Information is a provision of GDPR that would allow a customer to request access to their personal data and update it where needed. We need to garner more input on this provision to understanding it fully. Currently, we have no proposal for providing this capability electronically.

Other Related Items

Many of you are getting requests for bids and security surveys from your customers that include extensive questions on security of your data and networks.

For our customers being hosted in our standard Azure hosting environments, much of the responsibility for security of your data are shared between EWS Group and Microsoft Azure's security team. We will be continuing to take steps to secure our systems and your data to the best of our ability. This, at some point soon, may include penetration testing of multiple access points as well as following security guidelines laid out by the Microsoft Azure team. Securing your local networks will remain your responsibility.

For our customers working outside our Azure environment, the responsibility of securing your network is mostly yours. We will continue to do what we need to for MoversSuite, our APIs, and our other products, but we stress that overall system security is each of our customer’s own responsibility.

In the future, we plan to provide white paper that details as much information as possible regarding security. Our continuing goal is to give you information about what EWS Group is doing and to lay out our recommendations regarding security.

Closing Message

In closing, we really do believe that each of you should do your own research in to how GDPR affects you and your customers. For a long time, we assumed GDPR would have no direct impact on MoversSuite, since we have no customers directly in the EU. We have since learned otherwise. On our behalf, we have asked our corporate legal team to advise us on what changes may be needed in our contracts and the terms and conditions of our software. We will share with you the information we receive from those we consult with as well as what we learn internally, so that you and your customers can move forward in a more secure world.