GDPR: STATEMENT OF DIRECTION LN

INTRODUCTION: The GDPR

On April 27, 2016, the EU data protection regime (i.e., the European Parliament, the Council of the European Union, and the European Commission) expanded the scope of EU data protection law by adopting the **General Data Protection Regulation (GDPR)**.

The GDPR is a law designed to strengthen and unify data protection for all individuals in the European Union (EU). It places obligations on both Data Controllers and Data Processors.

The GDPR takes effect on May 25, 2018, and will supersede the existing data protection legislation (EU Directive 95/46/EC).

We recommend that our Customers assess the GDPR's impact on your organizational data processing activities.

INFOR'S OVERALL STATEMENT REGARDING GDPR and LN

The GDPR is a big law, and our overall product evaluation is a major undertaking. The continuing goal is to enhance LN's features and functionality in order to support our customers' efforts in meeting the requirements of GDPR, specifically, those that are applicable to LN.

PLANNED DELIVERIES FROM INFOR FOR LN

Below is a summary of the direction LN is heading in 2018. Product updates will be made available for versions LN 10.4, 10.5, 10.5.1, 10.5.2., 10.6 and up.

PRODUCT CAPABILITY	GDPR REFERENCE	WHERE WE'RE HEADED
ACCESS	**Article 15**	**Existing functionality:** Data Controllers can access and modify all data through regular sessions and functionalities. They can access data on behalf of Data Subjects and generate reports to provide information to the Data Subject.
RECTIFICATION OF INACCURACIES	**Article 16**	**Existing functionality:** LN customers have full capabilities to adjust and modify incorrect data. Access to data can be restricted to specific (groups of) users.
PERMANENT ERASURE (THE RIGHT TO BE FORGOTTEN)	**Article 17**	**Existing functionality:** Customers have the option to permanently

		delete data. The LN data model enables easy deletion of data. **Direction:** In LN, a new parameter is introduced that dictates if anonymization logic is available. Various sessions will get a new 'Anonymize' form command, requiring full authorization to be executed. In scenarios where permanent deletion is impossible because of referential constraints of the database, the user can apply the 'Anonymize' command which will erase privacy sensitive contents by overwriting it by a pre-defined anonymization character. The desired anonymization character can be defined in an additional system parameter.

RESTRICTION OF & OBJECTION TO PROCESSING	Articles 18 & 21	Existing functionality: Infor LN offers a multitude of functionalities to restrict access to data via Data authorization management. This can be based on specific tables, sessions & fields. Also, status control of numerous business objects and data fields.
DATA PORTABILITY (MACHINE-READABLE FORMATS)	**Article 20**	**Existing functionality:** All data can be easily exported via pre-formatted exchange schemes, Excel export, XML based middleware, API's etc.
AUTOMATED DECISION-MAKING	**Article 22**	**Not applicable.** There is no automated decision-making in the LN solution.
DATA RETURN OR DELETION	**Article 28**	**Existing functionality:** Infor LN customers can delete and/or archive all data without any restriction. Retention

		periods for archiving are available.
TECHNICAL & ORGANIZATIONAL SECURITY MEASURES	**Article 25**	**Existing functionality:** Infor LN provides the functionality to demonstrate the timeliness of issuing, suspending and closing user accounts through the option to log any transaction (e.g. end-user action) that occurred in user master data table (i.e. table: user data), such as granting and revoking access on the application layer. This data can be requested in the default system functionality 'audit report'. Infor LN provides the functionality to report all user access rights in various formats (i.e. print session authorizations by user) to allow for a periodical review and confirmation of user

		access rights by the user organization. Infor LN also provides the functionality to allow the user organization to monitor and log security events (i.e. failed logon and unauthorized access) by accessing the log file on the operating system). LN has a full role-based access control layered to restrict who can view/edit data. Audit trail capabilities also exist.
CONSENT	**Article 7**	Not applicable. There are no data processing activities that require consent via the LN solution.

INFORMATION ABOUT THIS DOCUMENT

Infor is a software developer and service provider, and not a legal advisor regarding the provisions of the GDPR; therefore, this document should not be construed as legal advice or a contractual commitment.
This document reflects the direction Infor may take with regards to the specific product(s) described in this document, all of which is subject to change by Infor in its sole discretion, with or without notice to you. You should not rely on this document or any of its content in making any decisions regarding your own compliance efforts. Infor's determination to develop or deliver any specified enhancement, upgrade, product or functionality, as described in this document, will be based on technical and commercial feasibility.