Table of Contents

CONTEXT

In May 2018 the new General Data Protection Regulation (GDPR) comes into force. The incoming regulation imposes new rules on organizations which offer goods and/or services to people in the European Union (EU), or which collect and/or analyse data relating to EU residents. Compliance with the GDPR is mandatory when 'processing' (collecting, using, storing, transferring) personal data of any EU citizen no matter where in the world the data is processed, and is also mandatory for any organization established in the EU.

VALIDIS – AN OVERVIEW

Validis Holdings Ltd ("Validis"), headquartered in London, UK, is a provider of software to manage the transfer of organisations' accounting data to financial institutions and accounting firms and the subsequent workflows performed by these institutions. This software is provided as a cloud hosted service. Validis has two main offices. Our headquarters located in London, UK and our North American office located in Austin, Texas.

DATASHARE – AN OVERVIEW

DataShare provides a data transfer and tooling platform for sending and receiving accounting data. Services offered include, but are not limited to:

- Extraction of General Ledger, Accounts Receivable & Accounts Payable accounting data from on-premise and cloud hosted accounting packages
- Standardization and normalization of accounting data across all data sources
- Custom multi-tenanted website for data submission management and analysis
- Tools to aid processes such as audit, management accounts monitoring and quality scoring
- Integrations with third-party applications to request data
- APIs allowing services to be integrated with third-party applications

BACKGROUND TO GDPR

The GDPR will strengthen, harmonize, and modernize EU data protection law and enhance individual rights and freedoms, consistent with the European understanding of privacy as a fundamental human right. The GDPR regulates, among other things, how individuals and organizations may obtain, use, store, share and delete personal data. It will have a significant impact on businesses around the world.

WHAT CONSTITUTES PERSONAL DATA?

While retaining much of the substance of the existing definition, the GDPR adopts a broader definition, which emphasizes the relevance of bio-metric and genetic information as an 'identifier' which could fall within the scope of 'personal data' (and therefore the new law). The GDPR states that "'personal data'

means any information relating to an identified or identifiable natural person… an identifiable natural person is one who can be identified directly or indirectly… by reference to an identifier… or to one or more factors specific to… that natural person". As such, any data by which an individual can be identified, whether based on the data alone, or when combined with other (reasonably attainable) information is likely to be included in the definition of 'personal data'. This now means that, as all the data which would normally be considered personal data for example name, email address etc., under certain circumstances it could also include IP addresses, mobile device ID's data as well.

Additional factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that individual are also given specific mention in the GDPR as potentially falling within the scope of the Regulation.

While the concept has long been the subject of guidance by the Information Commissioner's Office, for the first time, the legislation provides a definition of 'pseudonymous data' – personal data that has been subjected to technological measures (for instance, hashing or encryption) and makes it clear that, if this information may (without too much difficulty) be re-identified and linked back to any individual, it too will fall within the scope of 'personal data' notwithstanding the processes applied.

As with the DPA's regime, the GDPR acknowledges a second category of personal data which has been termed 'special categories' of personal data. Data types which are included in this category are racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership; data concerning health or sex life and sexual orientation; genetic data or bio-metric data. Given the potential for damage if such data was leaked or subject to unauthorized access, this type of data is required to be given even greater protection than other types of personal data.

TAKING DATA SECURITY SERIOUSLY

At Validis, we have always taken data security and data privacy extremely seriously. Our aim has always been to provide our customers with the highest level of data security and be accountable for the information held on our application. As such we regularly review and reinforce our security practices.

It is easy to claim compliance, but can be rather more challenging to demonstrate compliance on an ongoing basis. However, at Validis, we understand that being able to show our customers what we do is important, and we know it is exactly what is required under the GDPR. Validis, has for many years been certified against the ISO27001 security standard (most recently audited in October 2017) and earlier last year we were accredited SOC2 certification. We host our SaaS DataShare within the Microsoft Azure environment in the EU, US and Canada and Microsoft Azure is the most recognized Global Cloud Service provider, certified to ISO27001, SOC2 (among other security certifications).

We believe that the GDPR is an important step forward for clarifying and enabling individual privacy rights, and enforcing accountability. As such, we are committed to ensuring that we are GDPR compliant and want to make sure that in the services we provide to you (in your role as the 'data controller' – see below) we will be able to assist you to meet your obligations under the GDPR.

CONTROLLER OR PROCESSOR

The key distinction in understanding your obligations under the GDPR is assessing whether you are a data controller or a data processor. The controller is the organization that determines the purposes and means of processing personal data, as well as deciding what personal data is collected from a 'data subject' for processing. The processor is the organization that processes the data on behalf of the controller. Controllers will retain primary responsibility for data protection (including, for example, the obligation to report data breaches to data protection authorities); however, the GDPR does place some direct responsibilities on the processor, as well.

We act as a data controller in respect of any information which we collect about our customers.
We will never share this or any customer data in our possession with anyone else save as required at law or if we were to sell our business. Validis adheres to strict data security, access, integrity policies.

We act as a data processor in respect of any information which your customers upload onto DataShare.
In providing our service, we do not own or make decisions about the use of the information stored or processed on DataShare. We do not use this data for our own purposes. In fact, to the extent we do access it, it is only as reasonably necessary to provide you with our services (which may include responding to support requests) or as required by law. It is up to our customers to make sure that they comply with the relevant data protection legislation before uploading information to DataShare for processing.

In accordance with the GDPR, we have updated our terms of business so that we will only ever use personal data which we process on our customers' behalf in accordance with our customers' instructions (to the extent consistent with the functionality of DataShare). We also implement appropriate security, technical, physical and administrative measures against unauthorized processing of such information and against loss, destruction of, or damage to, personal information.

As part of our service, DataShare has the necessary functionality to enable our customers to push out their own privacy policy – if they are relying on consent as the legal basis for processing.

HOW DOES DATASHARE FACILITATE THE CORE PRINCIPLES UNDER GDPR?

Principle / Description	**How "DataShare" Facilitates compliance to GDPR**
Lawfulness, fairness and transparency *Personal data shall be processed lawfully, fairly and in a transparent manner.*	We only process data in a manner agreed as part of our client contracts. As part of our service, DataShare has the necessary functionality to enable our customers to push out their own Terms and Conditions/End User License agreement (EULA). All users must accept the Terms and Conditions/EULA before being granted access to the site. If the Terms and Conditions/EULA are not accepted, the user will be denied access to the site. Our clients will be able to maintain their Terms and Conditions/EULA within the system.

Purpose limitation *Personal data shall be collected for specified, explicit and legitimate purposes.*	DataShare only extracts the transaction & allocation history from the 3 core financial modules (General Ledger, Accounts Receivable & Accounts Payable), to be able to deliver the required reports and services for the performance of the contract with our Clients. The Purposes for which the Personal data is processed is specified in our contracts with Clients. Furthermore, as part of our service, DataShare has the necessary functionality to enable our customers to push out their own Terms and Conditions/End User License agreement. All end users must accept the Terms and Conditions/EULA before being granted access to the site. If the Terms and Conditions/EULA are not accepted, the user will be denied access to the site. Our clients will be able to maintain their Terms and Conditions/EULA within the system.
Data minimization *Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.*	DataShare extracts the full transaction & allocation history from the 3 core financial modules (General Ledger, Accounts Receivable & Accounts Payable). It copies the below information (where it is available and/or populated within the accounting application). • Company Information - Company Name, Address, Vat Number (or country/regional variation), Company Number • Contact Details (Phone, Fax, Email, Website URL) • Financial Year End • Accounting Application Name and Version • Transactional data from the General Ledger, Accounts Payable and Accounts Receivable. • Receivables and Payables information. • Chart of Accounts, with control account and category information. • Accounting period Information with nominal account opening/closing balances. In addition to the above, personal data such as Name, work contact information such as phone and email are required to be entered as part of the registration process. All the above data is necessary for Validis to provide the required services and reports via “DataShare”.
Accuracy	DataShare provides the capability for our clients and their customers (SMEs) to enter and update their Personal data on the application during registration and edit as necessary so the personal data shall be kept accurate and where necessary kept up to date. SMEs are

Personal data shall be accurate and, where necessary, kept up to date.	responsible to ensure any data uploaded on to DataShare is accurate and up to date.
Storage limitation *Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.*	Data, including any Personal data processed through DataShare is only kept as long as the contract with the client is active to provide the required services, and in the backups for a further 90 days in line with our backup policy. The data is then securely deleted and destroyed in an irrecoverable fashion.
Integrity and confidentiality *Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures.*	Data extracted from End User's accounting software is encrypted before transmission to the application. Validis is both ISO27001 and SOC2 certified, ensuring appropriate technical and organizational measures are in place to protect the data. Detailed information of these measures can be found in our Technical and security document.
Accountability *The controller shall be responsible for, and be able to demonstrate compliance with the GDPR.*	The DataShare Admin capability within the platform allows our Clients (data controllers) to take full control of their instance of the application including user maintenance and engagement management, providing them the required capabilities to ensure accountability of their user data, including any personal data.

HOW DOES DATASHARE FACILITATE THE RIGHTS OF INDIVIDUALS UNDER GDPR?

Rights / Description	**How "DataShare" Facilitates compliance to GDPR.**
Right to be Informed *(Articles 12, 13 and 14) of GDPR*	DataShare enables our client to define their own Terms and Conditions /End User License Agreements. Using this privacy statement, our clients are able to notify their customers/end users/SMEs of the details of personal data being collecting and the purpose. Within DataShare, the Client can make it mandatory for the

	SME to accept the terms before proceeding with registration to the system and if the terms are amended, to confirm acceptance of the amended terms.
Right to Access and Portability *(Article 15) of GDPR* *(Article 20) of GDPR*	Within DataShare, all end users can see and update the personal details held about them. DataShare allows our clients to manage their Customers data and users, including any Personal data provided by the end user/SME as part of their registration. providing them with full control to be able to supply the required information to their customers/end users.
The right to rectification *(Article 16) of GDPR*	Within DataShare all users can see and update their own personal details. Alternatively, client administrators can update an individual's personal details within the system.
Right to be Forgotten /Erasure *(Article 17) of GDPR*	DataShare enables our Clients to comply with an individual's request for the deletion or removal of personal data from the platform. If our customers are satisfied that there is no compelling reason for continued processing, they can delete the data from DataShare. DataShare provides our customers with full control on their end user data and user management providing options to disable and "soft" delete the data as requested by the end user/SME, supporting our clients to be able to erase their end user's personal data and cease further dissemination of the data.
The right to restrict/Object processing. *(Article 20) of GDPR*	Should an SME wish to object to the processing of their data on DataShare, the SME/End User's record/engagement can be disabled. The 'Disable" feature can be used to suspend processing until further notice.
Rights related to automated decision making and profiling. *(Article 22) of GDPR*	DataShare doesn't allow automated decisions or profiling within its platform.

HOW DOES DATASHARE FACILITATE THE OTHER KEY FACTORS UNDER GDPR?

Principle and Article	**How "DataShare" Facilitates compliance to GDPR**
Territorial Scope	DataShare is hosted on Microsoft Azure, one of the largest and most respected hosting and service providers in the world. The MS

(Article 3) of GDPR	Azure infrastructure puts strong safeguards in place to help protect customer privacy. All data is stored in highly secure MS Azure data centers (region depending on client requirements). Data is never transferred outside the region even for backup or DR purposes ensuring data sovereignty at all times. For all EU customers, data is hosted in the MS Azure data centers in the EEA.
Explicit and retractable Consent *(Article 4, 6 and 9) of GDPR*	The consent process is managed through the contract between Validis and our Clients. The DataShare platform further facilitates our clients in their consent with their customers/SMEs/end users by providing the capability to maintain their Terms and Conditions/ EULA within the system. All end users must accept the Terms and Conditions/EULA before being granted access to the site. If the Terms and Conditions/EULA are not accepted, the user will be denied access to the site. Our clients will be able to maintain their Terms and Conditions/EULA within the system.
Breach notification *(Article 33) of GDPR*	Validis is ISO27001 and SOC2 certified and employ appropriate security, technical and organizational measures to ensure the data is protected from unauthorized use and disclosure. This includes monitoring our systems and notifying our Clients of a personal data breach. For more detailed information on what security measures we currently employ, please refer to the Technical and Security Document.
Privacy by Design *(Article 25) of GDPR*	Privacy by Design is a legal requirement under GDPR and Validis take this seriously. DataShare is designed with both Security and Privacy in mind. A Privacy Impact assessment for DataShare was carried out as part of the GDPR project and this document provides a summarized version of that exercise.

FURTHER INFORMATION

If you have any further questions or queries with any of the details above, please feel free to contact us at privacy@validis.com

NOTHING IN THIS DOCUMENT IS INTENDED TO BE NOR SHOULD IT BE RELIED UPON AS LEGAL ADVICE. IT IS UP TO YOU TO SEEK LEGAL ADVICE IN RESPECT OF YOUR OBLIGATIONS UNDER THE GDPR.