rms
operational excellence

connect without compromise
metro

RETAIL MANAGER SOLUTIONS LIMITED

GDPR Position Statement

21st February 2018

Confidentiality

Retail Manager Solutions Limited (RMS) is committed to maintaining the highest degree of integrity in all our dealings with potential, current and past clients of RMS, both in terms of normal commercial confidentiality and the protection of all personal information received in the course of providing the business products and services provided by RMS.

RMS extends the same standards to all of our clients, suppliers and associates. We will comply with the legislative requirements with regard to confidentially and data protection and will ensure all our sub-contractors and third party suppliers (Sub Data Processors) agree and adopt our non-disclosure agreement and conditions for operating and processing our client data.

Ethics

We conduct our own services honestly and honourably and expect our clients (Data Controllers) and Sub Data Processors to do the same. Our advice, strategic assistance and the methods imparted through our services take proper account of ethical considerations.

Duty of Care

Through our actions and advice, we will always try to conform to relevant law and RMS believes that all businesses and organisations, including our own business, have a duty of care to avoid causing any adverse effect on the rights and freedoms of individuals.

Terms and Conditions

Our contract and/or terms and conditions of engagement will usually be in the form of a detailed proposal, including aims, activities, costs, timescales and deliverables. They are supported by our General Data Protection Regulation (GDPR) statement of intent (see below) in respect of our processing activities as a Data Processor / Sub Data Processor under the GDPR.

The quality of our products and services and the value of our service to our clients are paramount to us and RMS will always strive to meet our clients' contractual requirements. We shall ensure a compliance review is carried out against our own processing activities as a Data Processor / Sub Data Processor when supplying software products service solutions to our clients and ensure that all our Sub Data Processors do the same.

Intellectual Property & Moral Rights

RMS retains the moral rights in, and ownership of, all intellectual property that we create unless agreed otherwise in advance with our clients. In return we respect the moral and intellectual copyright vested in our clients' intellectual property. Our suppliers are under strict terms of confidentiality not to disclose, disseminate and/or inform any third party about RMS’ clients, business or individual (data subjects) personal identifiable information.

Quality Assurance

RMS maintains the quality of what we do through constant ongoing review with our clients, of all aims, activities, outcomes and the cost-effectiveness of every activity. We encourage regular review meetings and provide regular progress reports on the services we are engaged to deliver.

Professional Conduct

RMS endeavours to conduct all of our activities with professionalism and integrity. We take great care to be completely objective in the judgement and any recommendations that are proposed, so that issues are never influenced by anything other than the best and proper interests of our clients.

Diversity, Equality & Discrimination

RMS always strives to be fair and objective in our advice and actions. We practice compliance with all forms of discrimination legislation, and actively promote policies and procedures to ensure that no person is ever disadvantaged by reason of their racial or ethnic origin, or on grounds of gender, sexual orientation (including gender reassignment), marital status, age, nationality, religion or belief or disability or any action which may constitute harassment of any kind.

General Data Protection Regulation Statement

This 'position statement' sets down our approach with regard to compliance with our obligations under GDPR in relation to:

- our products , services and data storage;
- as a Data Processor on behalf of our customers; and
- as a Data Controller for the purposes of:
    - processing our employee data for our own accounts and purposes; and
    - promoting our products and services through marketing.

The role of the Data Processor is the processing of the data under the instructions of the Data Controller, (our clients). Under the GDPR, RMS will:

- Provide software solutions which allow our clients, as Data Controllers, to process and store the Personal Identifiable Information (PII) of their data subjects.
- As a Data Processor, embed in our approach the principles of the "Privacy by Design" (PBD) requirement when creating, designing a new, or maintaining an existing, software and/or storage solution.
- If the software or services is used for the handling of PII, ensure it will follow the principles of PBD.

Privacy by Design and Software and Service Development Life Cycle

As a software and service provider RMS, as a Data Processor, supports PBD principles in delivery of a solution, whether it be out-of-the-box or is uniquely configured or a customised solution. The software and services provided by RMS will follow our own software and Service Development Life Cycle (SDLC) and corresponding IT development processes to cover the lifecycle of an information system which holds PII:

I. Plan;
II. Design;
III. Build;
IV. Test;
V. Rollout; and
VI. Maintain.

RMS is fully aware that as a Data Processor we need to support our clients as Data Controllers. There are key areas of data management and protection relevant to the GDPR Articles and Recitals which influence the SDLC's functional and technical planning requirements in regard to adopting a PBD approach when implementing data protection into the system and organisation as a legal requirement.

We understand under **Article 25-1/3** our clients, as Data Controllers, shall determine the means of processing as well as the risks of varying likelihood and severity for the rights and freedoms of an individual and in doing so they need to implement appropriate technical and organisational measures for security when it relates to PII as much as for pseudonymisation data sets.

Under **Recital 78** our clients, as Data Controllers, will be required to demonstrate compliance to adopt and implement measures which meet the Principles of data protection by design and data protection by default. Among other things, transparency will need to be demonstrated with regard to functions and to enable the individual (data subject) to monitor the data processing, enabling proper security controls are in place.

Where developing, designing, selecting and using applications, products and services that are based on the processing of personal data or the processing is necessary to fulfil a task, RMS, as a Data Processor, will take account of both the rights of individuals and the GDPR obligations of their clients as Data Controllers when developing and designing our products, services and applications. This will include performance of Privacy Impact Assessments (PIAs) with regard to our products and services for general application. However clients should note that such PIAs will not be specific to a client's use of personal data that it may hold as a Data Controller, for which the client alone must perform its own PIA when deploying RMS software and services to comply with **Articles 23 and 25**.

Data is secured, and the integrity and confidentiality are maintained, using technical and organisational means under the management of our client as a Data Controller when they position the software solution or product inside their own IT infrastructure. When using RMS data centre or storage services, RMS may use the services of a third party (Microsoft Azure, Amazon Web Services) which is as an EU based company and will act as a Sub Data Processor of RMS. When we use Sub Data Processors, RMS will ensure full compliance required under the GDPR is observed as follows:

Article 5.1(f)
Personal data will be processed in a manner that ensures appropriate security, protection against unauthorised or unlawful processing and against accidental loss, destruction or damage. Using appropriate technical or organisational measures ('integrity and confidentiality).

Article 24
To support where applicable the responsibility and liability of a Data Controller in the requirement of responding to any risk or security assessments in regards to the processing of PII in relation to their data subjects. It is understood by RMS that the role of the Data Controller is to ensure appropriate technical and organisational measures are in place to ensure and demonstrate compliance and are

regularly reviewed. As referred in *Article 42* adherence to approved codes of conduct and/or approved certification mechanisms may be used as an element of demonstrated compliance.

Article 32-1 (b-d)
It is the Data Controller's responsibility to i) ensure ongoing confidentially, integrity, availability and resilience of processing systems and services; ii) restore and make available or accessible personal data in a timely manner in the event of a physical or technical incident; and iii) regularly test and evaluate the effectiveness of the technical and organisational measures for security.

Recital 49
The processing of personal data to the extent strictly necessary and proportionate for the purposes of ensuring network and information security, i.e. the ability of a network or an information system to resist, at a given level of confidence, accidental events or unlawful or malicious actions that compromise the availability, authenticity, integrity and confidentiality of stored or transmitted personal data, and the security of the related services offered by, or accessible via, those networks and systems, by public authorities, by computer emergency response teams, computer security incident response teams, by providers of electronic communications networks and services and by providers of security technologies and services, constitutes a legitimate interest of the Data Controller concerned. This could, for example, include preventing unauthorised access to electronic communications networks and malicious code distribution and stopping 'denial of service' attacks and damage to computer and electronic communication systems.

RMS will assist their clients if they require a system configuration with regard to data encryption or pseudonymisation. **Article 6 – 4(e)** states a Data Controller shall take into account the existence of the appropriate safeguards, which may include encryption and pseudonymisation. **Article 32-1(a)** states a Data Controller and Data Processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk including amongst other things as appropriate for the pseudonymisation and encryption of personal data.

Under GDPR **Recital 26** it clearly states the Data Controller needs to abide by the Principles of data protection and that this should apply with regard to PII which has undergone pseudonymisation, where if it is attributed to an individual by the use of connecting information would be considered PII. To ascertain whether means are reasonably likely to be used to identify the individual, account should be taken of all objective factors, such as costs of the amount of time required for identification, taking into consideration the available technologies at the time of the processing and their developments.

Recital 28 - The application of the pseudonymisation to personal data can reduce the risks to the data subject; explicit introduction of 'pseudonymisation' in the GDPR is not intended to preclude any other measures of data protection.

Recital 29 - The purposes are to create incentives to apply pseudonymisation as a practice when processing PII. The GDPR is implemented in such a way that additional PII to a specific individual (data subject) is kept separately. The Data Controller processing the PII should indicate the authorised person within the same controller, for example separate departments. The Data Controller should also remove all PII indicators when processing data and ensure no link can be made to reconstitute the data back to an individual (data subject).

Under the **Recital 83,** the Data Controller and Data Processor should evaluate the risks inherent in the processing and implement measures to mitigate risks, such as encryption. Appropriate security measures such as confidentiality, to ensure consideration is applied to the risks such as accidental

loss, unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed which may lead to physical, material or non-material damage to an individual(s).

As detailed in **Recitals 39 and 58** the principle on transparency makes it clear that our client, as a Data Controller, is required to meet their obligations and RMS shall, as their Data Processor, will assist our client to meet their obligations.

The products and services which hold and process PII will be required to comply with the **GDPR Principles** and the rights of individuals (data subjects).

The *right to port data* is a complex matter, and needs a case by case review, but system holding data would have the ability to allow a Data Controller to make that determination. As much as to meet **Article 20** where a Data Controller has to supply an individual with a copy of their data in a structured, commonly used and machine-readable format and the individual has the right to 'port' that data without hindrance or delay. An individual has a right to require one Data Controller to transmit the data pertaining to them to another Data Controller where technically feasible. We will assist in supplying secure access or transmission solutions if the data porting applies to data we hold in our hosted environments.

We understand that our clients, as Data Controllers, have to inform all Data Processors where the individual's data is processed by IT / Applications / Storage systems that the individual has exercised their *right to erasure*. Controller and Processor inventories are critical to this right and in doing so RMS will co-operate with our clients to fulfil this obligation. To this aim and under **Article 19** our clients, as the Data Controller, will inform us as the Data Processor or Sub Processor where the *right to rectification /erasure / restriction* have been exercised by the individual. The exemption to this is if it involves disproportionate effort. The Data Controller will inform the individual of all the recipients with whom their data has been shared and under **Recital 66,** where our Client as the Data Controller have shared individuals PII with RMS, will inform us as the Data Processor that such right has been exercised and the data subject's PII is to be erased in any links to, or copies or replications of the personal data.

Data Breaches

For the purposes of processing of PII which may result in a contravention of the GDPR (a data breach), RMS, as the Data Processor, and/or our Sub Data Processors, will determine if i) a breach is likely, and ii) there is a high risk to processing of the PII in the systems held outside of our clients IT infrastructure (e.g. hosted by our third party Sub Data Processors,) which could put at risk the rights and freedoms of data subjects, and we will ensure such technical measures are in place to identify, track, assess and report such breaches. We will report all contraventions with regard to data security to our clients as Data Controllers.

Where our client requires us as the Data Processor or our Sub Data Processor to carry out activities which could lead to a contravention of GDPR, we as Data Processor and our Sub Data Processors reserve the right to refuse such processing activities.

Such security measures and reporting of data breaches will be dealt with in compliance with GDPR and in particular, **Articles 33 and 34** and **Recitals 85, 86 and 87**. This includes addressing the reporting obligations to the individual (data subject) as well as to the Information Authority in the member state where the data is held and processed.

RMS as a Data Processor

A Data Processor is defined in **Article 4(8**) as a natural or legal person, public authority, agency or other body which processes personal data on behalf of the data controllers. Under the GDPR **Recital 81 1-10 (a-h),** a Data Controller shall only use Data Processors who provide sufficient guarantees to implement appropriate technical and organisational measures in order that their processing activities will meet the requirements of the Regulation and ensure the protection of individuals rights (data subject).

Engagement of Sub Data Processors and contractual obligations

It is understood by RMS, as a Data Processor, that we shall not engage a Sub Data Processor without the prior specific or general written authorisation of our clients as Data Controllers. Where RMS and/or the client as a Data Controller require services from a Sub Data Processor, each will consult and require demonstration of compliance under the GDPR by the Sub Data Processor. This will be in writing and each party will demonstrate compliance and record such in the contract and record any intended changes concerning the engagement, replacement or addition of a Sub Data Processor allowing time for the parties to object and/or agree.

A Data Controller will require a full report and set of evidence from the Sub Data Processor with regard to compliance with the GDPR as part of the written notification and will have the right to audit the main Data Processor as much as the Sub Data Processor. It is therefore understood by RMS that the relationship between their clients as Data Controllers and RMS as the Data Processor and our Sub Processors will be governed by a contract or other legislative laws in the EU or as part of UK law that is binding on the Data Processor / Sub Processor. The contract will set out, as a minimum:

- the subject matter,
- duration,
- the nature and purpose of the processing,
- the types of personal and sensitive categories of data; and
- the categories of data subjects.

It will also define and set the obligations and rights of the Data Controller. The contract or other legal agreement shall provide, in particular, that the Data Processor and any Sub Data Processors:

a) only process data on documented instructions from the Data Controller, and do not transfer any personal data to a third country or international organisation, unless required to do so by Union or Member State law to which the Data Processor and/or Sub Data Processors are subject (in these circumstances the Data Processor shall inform the Data Controller of such legal requirement before processing, unless the law prohibits such information on important grounds of public interest);

b) ensure that persons authorised to process the data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;

c) take all measures set out in **Article 32 Security** of personal data;

d) respect the conditions to bring in and use a Sub Data Processor and in doing so will ensure a specific written agreement is in place with the Data Controller and that the Sub Data Processor follows the same contractual conditions and obligations as the main Data Processor

and in doing so is liable under the same contractual agreements for any breach of such agreement. Where the Sub Data Processor fails to fulfil its data protection obligations, the Data Processor shall remain fully liable to the Data Controller. Both Data Processor / Sub Processor shall provide sufficient guarantees to implement appropriate technical and organisational measures to meet the requirements of the GDPR. The Information Authority (Supervisory Authority) may adopt a standard contractual clause(s) for such purpose as set down in **Article 63**;

e) assist the Data Controller in a timely manner in all matters pertaining to the response and processing of data with regard to data subjects' rights;

f) assist the Data Controller by i) ensuring data is kept secure, ii) notifying the Data Controller of any potential or actual breach, and iii) assisting the Data Controller with any information to inform any affected individual;

g) ensure full documentary evidence is in place to show that all data provided to the Data Processor and/or Sub Data Processor has been destroyed, unless Union or Member State Law requires storage of the personal data;

h) allow the Data Controller the right to audit and to evidence compliance with the obligations laid down under the GDPR, including audits by the Data Controller or their chosen authorised agent;

i) work with the Data Controller with regard to any consultation with the Information Authority (Supervisory Authority);

j) are permitted the right to inform the Data Controller if, in their opinion, an instruction from the Data Controller infringes GDPR or other Union or Member State data protection provisions.

RMS as the Data Processor will not make any determination of the use of their clients' PII as in doing so it would mean we would be considered to be a Data Controller.

Liability and Right to Compensation

Under **Article 82,** *the right to compensation*, any data subject who has suffered material or non-material damage as a result of a breach of the law shall have the right to receive compensation from the Data Controller and Data Processor for the damage suffered. The Data Processor shall be liable for the damage caused by the processing only where it has not complied with the obligations of the EU GDPR, Union and Member State Law. The Data Processor as much as the Data Controller shall be exempt from liability if they can prove that it is not in any way responsible for the event giving rise to the damage.

It is understood by RMS that either alone or jointly both the Data Controller and the Data Processor can be found liable for the entire damage in order to ensure effective compensation of the data subject affected. Where the Data Processor has paid full compensation for the damage suffered, it is entitled to claim back from the Data Controller or other Data Processor that part of the compensation corresponding to their part in the responsibility for the damage (**Recital 50)**.

Legal action via the courts can be pursued by the damaged individual under the law of the Member State. The general conditions to impose fines will be managed by the applicable Information Authority

in the country where the data subjects' data is processed and/or where joint Information Authorities agree which concerned Authority will take the lead.

Other data protection legislation

RMS have also taken note of the UK **Digital Economy Act** (DEA) as part of their GDPR compliance review and strategy as it covers a variety of different measures, one of which is the requirement to register with the Information Authority which will be based on the volume of data they process and the category of the data. This is yet to be translated by the Information Commissioner's Office in the UK but it is noted by RMS as a Data Controller processing employee and marketing data.

There are requirements for Data Controllers and Data Processors to ensure effective cyber security controls and awareness are in place. It brings in 'Directors Responsibility', which means personal liability of company directors for infringements of the Regulation and the forthcoming **UK Data Protection Act 2018** of which the GDPR will form part. The DEA brings about the requirement to ensure compliance with the Regulatory Information Sharing Code of Practice with regard to public sector data sharing. RMS will consider this code as part of their GDPR Strategy.

As part of our GDPR compliance review and strategy we have considered the **Data Protection Bill**, as the Bill exercises a number of agreed modifications to the GDPR to make it work for the UK. We shall be considering the requirement with regard to data transfers of PII to non-EU countries (section 17) which restricts the sharing of data to a non-EU country or international organisation which cannot demonstrate adequate protections as set out in **Article 45(3)**.

Special Categories of Personal Data (formally referred to as "sensitive personal data") needs to be justified for processing without consent for employment and criminal convictions purposes – RMS may process such data for such purpose as an employer, and also as a software and service provider as part of a system which will hold this data.

Age of consent to process children's data as in the provision of information services (internet/social media/gaming), where it is proposed to be reduced from 16 years under the GDPR to 13 years under the UK Data Protection Bill 2018. Those under 13 will need parental/guardian consent: RMS will require their clients as Data Controllers to confirm consent prior to any processing activity being carried by RMS and our Sub Data Processors.

We have also taken note of the change in the Data Protection Bill to bring about under English Law the new offences of intentionally or recklessly re-identifying individuals from anonymised or pseudonymised data and the altering of records with the intent to prevent disclosure.

Our Approach

RMS is working towards a programme of change to implement the GDPR with regard to our products and services. RMS offer a set of software and service systems to the Retail, Health, Leisure, and Hospitality Sectors, and it is acknowledged that some of our solutions hold a volume of personal and special categories of data.

Where our solutions are deployed and sit within our clients' IT infrastructure, they are protected by and under our clients IT, Information Security and Data Protection compliance controls. Where our

solutions are hosted by RMS we shall comply with this position statement and the provisions of GDPR and the forthcoming UK Data Protection Act 2018.

While RMS is not required to have a Mandatory Data Protection Officer under GDPR, we have decided to appoint one on a voluntary basis.

You are also referred to our GDPR product Statement found on the RMS website which gives more details in relation to GDPR compliance and our software products.