SYNERGY MARKETS LIMITED

GDPR & SENSTIVE DATA HANDLING POLICY

Status: *Internal document*

Audience – **ALL STAFF**

Pertaining to: Synergy Markets Limited - Companies House No.0884 3450.
Registered Office – Chiltern House, 45 Station Road, Henley-on-Thames, Oxfordshire, RG9 1AT

FCA number ('FRN') – 623190

ICO Registration – A8263266

Data Protection Officer ('DPO')– Mr Stephen Meli

Contact Number – 0203 868 8821

Contact e-mail – stephen.meli@synergy-markets.com

GENERAL

What is the GDPR?

From **25 May 2018,** the General Data Protection Act (GDPR) replaced the Data Protection Act 1998 (DPA) which governs the processing, handling and storing of personal data.

Why did it come into being?

The GDPR was a response to a number of factors:

i) An increasing prevalence of unwanted/nuisance marketing communications, via e-mail, SMS, and phone calls.

ii) An increasing and related awareness on the part of individuals – be that as ordinary citizens or businesses – that data was being collected and utilised, both legitimately and non-legitimately, for new and left-of-field purposes (e.g. adverts that seem uncannily tailored to websites visited, or location)

iii) Corporations and businesses 'addressing' the already-existent Data Protection rules through large tracts of text and 'legalease' – meaning that the individual is unlikely to either read through or comprehend their rights, and what is about to be done with their information. E.g. matters such as 'consent' and 'what consented to' were left unclear. So the GDPR has demanded concision and clarity in all relevant communications and policies

What does it require of businesses?

Below is a summary of what the GDPR actually means for businesses at ground-level. There is a slight caveat in that the emphasis and obligations can vary

1. Document the data that you hold, where the data came from and who you are sharing it with.

You should only process accurate personal data and any outdated or imprecise personal data should be deleted or updated. As a business, you are responsible for the personal data you manage and for the data that you provide to third parties. This means that if you pass on incorrect personal data to a third party, you are responsible for not only correcting the personal data you hold but informing the third party that they also need to update their data too.

Personal data must also be removed, destroyed or anonymised once the purpose for collecting the personal data has been fulfilled, for example, a project or contractual relationship where you have received personal data has ended (unless you have another lawful reason for keeping it).

Review your existing data and ensure that you know:

- what personal data you have;
- why you have it;
- where it is;
- who else has access to the personal data, and;
- how you got it in the first place,

is the first step to ensuring that you are ready for 25 May 2018.

2. Understand the lawful basis you will rely upon to hold the data

After you have a strong understanding of what data you have and what you use it for, you must then consider the lawful basis you will rely upon to retain the data. After 25 May 2018, you will only be permitted to hold data that is necessary and relevant to the purpose you need it for and you will need a lawful basis for holding the data.

It may help to compartmentalise your data in order to establish separate legal bases for each category. Typically, a business will hold data on its clients/customers and its employees. It may also hold data on past clients/customers, on potential employees if it is recruiting, on past employees and on other businesses or individuals for marketing purposes. Please note that this list is not exhaustive as each business is unique and the categories you choose will be specific to your business.

There are **six** lawful ways to hold data, these are set out in Article 6(1) of the GDPR and are as follows:

a) Consent

GDPR sets a high standard for consent but often you won't need it for most of the categories of data set out above. If you do need consent, you should ensure that consent is clear and concise, in plain language, and avoids the use of confusing terminology or legal jargon. Pre-ticked boxes or other methods for default, or opt-out, consent will no longer be valid. Under the GDPR, individuals must opt-in for you to be able to process their data.

If you use this legal basis for processing data then bear in mind that individuals can also withdraw consent at any time and they should be told this at the time of consenting.

When asking for consent you should include:

1. Purpose of the processing and the legal basis for the processing;
2. An active opt in clause;
3. The name of your organisation;
4. The name of any third party who will rely on the individual's consent to use the data;
5. On what basis you need the data;
6. What you will use it for;
7. How long you will retain the data for.

b) Contract

You will have a legal basis to hold data where it is deemed it is necessary to give effect to a contract. For example to supply goods or services that a client has requested, to fulfil a contract of employment or to pay a third party.

c) Legal obligation

If you are required under English or EU law to process data for a specified purpose you will have a lawful basis.

For example, if you have a contract with a client to provide services and you have subsequently provided those services and the contract has ended, you may no longer have a lawful basis upon which to hold their data. However, if you have an obligation to comply with a regulatory body or an insurance policy to retain client data for a period of time after you have provided the services, you may be able to rely on this lawful basis for retaining the data after the expiry of the contract.

d) Vital Interests

This basis is limited in scope and only applies if the processing of the data is necessary to protect someone's life. The Information Commissioner's Office states that this generally will only be relied upon in cases of 'life and death,' for example emergency medical care.

e) A Public Task

This is not likely to be relied on by small businesses or founders, as it relates to public bodies. For example if a public body needs the data to carry out official functions or a task in the public interest, then this will be a lawful basis.

f) Legitimate Interests

This is important in private sector organisations as you are able to process personal data if you have a genuine and legitimate reason, for example a commercial benefit or to fulfil an obligation. You must however ensure that there is no unwarranted impact on the individual i.e. it does not harm their rights or interest.

A commercial benefit is not usually considered sufficient to hold data for marketing purposes. For example, in the specific context of email marketing, holding an email address for the sole purpose of sending marketing emails does not fall under this as there is no certain commercial benefit for either party. The general consensus with regards to marketing is that it is safest to obtain consent.

Once the purpose has been fulfilled, the lawful basis will expire and the data should either be deleted, or anonymised, unless there is another lawful reason for keeping it (for example to comply with your insurance policy, legal obligations or other regulators).

3. Ensure that the data you hold is accurate, up to date and stored securely

As discussed above, you should only hold personal data, for a specific purpose. This supports the concept of data minimisation – the less data you have, the easier it is for it to be accurate and up to date.

You are responsible for the personal data you hold. You must therefore securely protect the data from theft, loss or misuse.

The way that this is done can vary and can be proportionate. The following is a helpful checklist:

- Ensure strict rules are in place for who can access what data and when. Create passwords and files for specific data, for specific purposes, and ensure that all employees understand the importance of it. For example, only the person who needs access to your employees' data should be allowed access to it.
- Data should be encrypted at every opportunity if it is stored on a computer, and if data is stored in a cloud-based system try to implement user-managed keys to provide an extra level of security for more sensitive data.
- If you hold hard copies of data, ensure that this is organised, that you can easily locate all the information that you need and also keep track of copies that may be made.
- Make sure that documents are kept private, having personal data on office walls for example, may constitute a breach. This is especially important if you work on paper files as transportation of this data should be very carefully considered given the evident threat to the security of such information.

4. Check your existing third-party contracts (e.g. when outsourcing payroll/HR/IT/marketing services to another company)

If you currently employ a third party to process personal data (data processor) on your behalf, then you should already have a written contract in place in order to comply with the DPA. However, under the GDPR, data controllers (your business) can be directly held liable for non-compliance of data processors so it is important to ensure that third parties who have access to your data are also GDPR compliant.

Steps to take:

- Identify all third parties who have access to personal data you have provided them with or who have access to personal data you hold;
- Make sure your data processor understands the reasons for the changes and the new obligations it has under the GDPR as well as the possibility of being

subject to an administrative fine or other sanction if it does not comply with its obligations;

- Review your current contracts and ensure wording is included to reflect the new GDPR contracts requirements and also that definitions are updated to align with the GDPR definitions. Additional wording should cover details of how data is processed and the processor's obligations (including the standards the processor must meet when processing personal data and the permissions it needs from you in relation to the processing);
- Make sure both you and your data processor are clear about your role in respect of the personal data that is being processed and that you can evidence this.
- You should also add a clause to cover what the third party should do in the event of a data breach. The general rule is that they should notify your business upon discovery of a breach as soon as is reasonable and at the latest within 72 hours.

5. Ensure that you have a procedure in place to detect, report and investigate data breaches

A data breach is a serious matter, even in a small business. Therefore having a procedure in place in case something does go wrong is critical.

You should know how to recognise a personal data breach, which includes understanding that it is not only about loss or theft of data, but also misuse of that data. In short, it can be defined as a security incident that has affected the confidentiality, integrity or availability of personal data. For example, if your IT system is hacked, or somebody accesses personal data without authorisation. You should have a procedure in place to deal with this in a timely and organised manner.

If the breach is likely to risk the rights and freedoms of the individuals whose data you hold, then you must notify the Information Commissioner's Office without undue delay and within 72 hours of your business becoming aware of the issue, even if you do not have all of the information about how it happened at that point.

This disclosure must include details on the individuals concerned, the likely consequences of the breach, what measures have been or will be taken to deal with the breach and the volume of data concerned.

SPECIFIC

Our business in the context of GDPR

We are an Investment services firm – assisting our clients with and advising on various investment opportunities, quandaries and decisions.

GDPR Culture - Management and staff awareness and responsibility

We are as a Company fully committed to both the letter and spirit of the GDPR – as summarised above under 'Why did it come into being?'. We equally expect all staff not only to comply with the policies and protocols as outlined in this document, but also to feel free to report breaches and anything else which they might be concerned by, in the context here of the GDPR/sensitive payment data. As a business – all staff are a key part of our overall approach to data security, all staff are our eyes and ears in this sense. We have a named Data Protection Officer (Stephen Meli) specifically so that you know whom to turn to with any concerns. You must also not hesitate if you think an incident might be 'damaging' to the Company – we would rather know about something and address it head-on, than have it buried out of the fear of the consequences. On the contrary – if you bring 'bad news' to the DPO – you have commendably not only done your job, but also played a crucial role in allowing the business as a whole to be and remain GDPR compliant. Remember – compliance is just as much about how we deal with things when they go wrong, as endeavouring not to have them go wrong in the first place.

FCA/TCF

As an FCA-Regulated firm – we are also subject to a set of core principles called Treating Customers Fairly ('TCF'). The GDPR is being regarded as a *de facto* extension of this – and so compliance with GDPR ties in with operating well as an FCA-Regulated firm.

GDPR Counterparties

The counterparties in our GDPR picture are:

i) Customer/client (= Data Subject)

ii) Investment destination/fund (= Data Processor)

It is primarily the 'Customer' above, from whom we glean data which could be classified as Sensitive (for KYC). It is Sensitive insofar as it entails ID and other documents (risks analysed below) – and it is *not* Sensitive Payment Data.

GDPR Roles

In our business model we undertake the role of a *Data Controller* under the GDPR definitions.

The payment services portal we use – Money Transfer Manager – would be classified as a sub-Controller, downstream of us. We would ensure that we are happy with their processes and procedures in terms of protecting the data which we as Data Controllers cause to be input onto their systems.

ICO Registration

As a Data Controller the business does require ICO registration (details on first page).

GDPR Contracts

We will if appropriate and necessary ensure that GDPR-specific Contracts exist between ourselves and any appropriate counterparties. The purpose of these are to enumerate and bi-laterally agree the respective roles we play under the GDPRs, in the normal course of business.

GDPR Data Categories

The data which we receive/handle in the course of business typically comprises the following categories:

i) Name and surname
ii) Proof of ID - photographic
iii) Proof of address (e.g. utility bills)
iv) Date of birth

v) Driving licence
vi) Passport – copy of photograph page

Data-type risk category

The risk-category has been deemed – **MEDIUM**

This is because the consequences of unauthorised release of or access to such information are greater than non-consequential, but do not create risks or scenarios whereby the data subject is at high risk of harm. One chief risk has been assessed as being identity theft, or fraudulent creation of credit card or bank accounts. This risk is limited in that the data subject would likely become aware of any such activity, as the address is used to verify identity.

We have not undertaken a Data Protection Impact Assessment as the deemed risk of a breach is not High.

Legal Basis

We will in the course of business only hold personal data which is necessary and relevant for the purposes of our business and specifically – the execute our duties as a business, in our capacity as a Data Controller.

The specific GDPR legal bases for our holding and processing personal data are:

i) *Necessity* – Our function/service cannot be executed without access to said data, especially given regulatory/AML/KYC obligations to ascertain and obtain much of it.

ii) *Legitimate Interests* – This ties in with the above

We would dispose of the data in question once our business relationship has been ended for a period of six months.

We will keep the data for the period of time during which the Data Subject is a customer of ours.

Data flow

This data is not shared with anyone other than the financial institution which the customer has chosen to do business with.

Data breaches

Data breach management comprises:

i) Processes to spot or become aware of data breaches
ii) Processes/protocols for these to be reported by staff
iii) Processes for other interested parties to be made aware of any such breaches or suspected breaches (Data subject)
iv) Our role in assisting to put things right for the data subject after any breach
v) Analysis of the basis for the breach, and implementing fixes to eliminate or further-minimise the chances of such a breach occurring again
vi) Staff disciplinary policy to take specific account of misdemeanours as regards GDPR

Data breach reporting

Serious breaches must be reported to the ICO. This includes an obligation also to inform any affected counterparties.

IT security

Our IT infrastructure is entirely derived from our IT services provider.

GDPR staff data

Below is the data that the business holds on all staff:

i) Full residential address
ii) National Insurance number
iii) Passport number
iv) Contact phone

v) E-mail address
vi) Next-of-kin – and contact details
vii) Sickness leave records
viii) Disciplinary records

Staff rights

Your rights are the same as those afforded ordinary individuals/consumers under the new data protection rules.

The DPO and all Management fully acknowledge these rights of yours, and you should not feel reticent about using them.

Right of access
You have a right to request and obtain sight of these records

Right to rectification and data quality
You have a right to ensure that the personal data we hold remains accurate and up to date

Right to erasure, including retention and disposal
These rights exist, and exist also in line with your employment contract.

Right to restrict processing
You have the right to request that we cease to utilise data any manner you disagree with – subject only to the business being able to process your data in a manner which allows you to execute the function for which you were/are employed, and for the business to maintain its own legal and fiduciary obligations surrounding your employment

Right to data portability
We are obliged to provide you your data in an electronic format.

Staff Process

If you have any concerns or requests, please speak to the Data Protection Officer.

END.