SERENA FORDHAM ENTERPRISES LTD, FOR HER GROUP LTD & NORFOLK MUMS

Data Protection Policy

DATA PROTECTION POLICY

Table of Contents:

1. Document Control

Document owner	Serena Fordham Managing Director and Founder
Prepared by	John Fordham Glow Virtual Assistants Operation Manager
Reviewed by	Serena Fordham Managing Director and Founder
Approved by	Serena Fordham Managing Director and Founder
Approved on	1st May 2018 (Updated 30th October 2018)
Next review date	1st April 2019
Reference	DPP_002
Version	1.0
Classification	Public

Distribution list	
Managing Director	To approve and authorise
All Staff	To understand and comply

Communication	The Data Protection Policy is communicated to all members of staff via email and data protection awareness training.

2. Introduction

Serena Fordham Enterprises Limited, For HER Group Limited and Norfolk Mums ('The Companies') is registered with the Information Commissioners Office (ICO).

The Companies recognise the General Data Protection Regulation (GDPR) and will endeavour to ensure that all personal data is processed in compliance with this regulation from 25 May 2018, the date the regulation comes into force.

This Data Protection Policy is written specifically to ensure appropriate compliance with the GDPR and has used the ICO self-assessment guidance for small organisations as at February 2018 for guidance as to the requirements.

The Companies have adopted the GDPR compliance requirements of the 'Data Controller' and 'Data Processor'.

3. General Statement of The Companies Scope

The Companies process relevant personal data regarding their members of staff, their clients and their client's customers, or their client's prospective customers, as part of its operation and shall take all reasonable steps to do so in accordance with this Policy.

Should the scope of the business undertaken by The Companies change, this Policy will be updated to reflect the changes in relation to compliance with the GDPR.

The Companies only operate within the European Union.

4. Contracts with Data Controllers

The Companies maintain signed contracts with its clients who are operating as Data Controllers under the GDPR for the purpose of this Policy.

The Companies / client contracts grant The Companies the ability to use sub-processors for the processing of some personal data related tasks such as email marketing.

5. Contracts with 3rd Party Data Processors

The Companies use 3rd party data processors such as those specialising in email marketing. The Companies have signed up to the standard contractual requirements of these processors. Such processors are striving to be GDPR compliant and are only based within the EU.

6. Data Protection Officer

The Companies have not appointed a Data Protection Officer as it is not required to do so under the GDPR.
Rather, each member of The Companies staff is expected to understand and comply with this Policy whilst undertaking the processing of personal data.

7. Data Protection Training

The Companies undertake appropriate and reasonable data protection training with its employees. The training focuses on the practical, day to day aspects of data protection in the context of the GDPR.

The training is provided for all employees as a dedicated training session during periodic team meetings. Staff not attending are provided with separate training as appropriate.

8. The Principles

The Companies shall so far as is appropriate and is reasonably practicable comply with the GDPR principles contained in Article 5 of the regulation which sets out the main responsibilities for organisations. These state that personal data should be:

a) processed lawfully, fairly and in a transparent manner in relation to individuals;

b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;

c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;

e) 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; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and

f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

9. Personal Data

Personal data covers facts about an individual where that data identifies an individual. For example, it includes information necessary for:

- employment such as the member of staff's name and address and details for payment of salary.;

- raising of client invoices for the payment of activity undertaken on behalf of the client; and
- the identification of client's customers and prospective customers for marketing purposes.

10. Processing of Personal Data

Consent may be required for the processing of personal data unless processing is necessary for the performance of the contract of employment. Any information which falls under the definition of personal data and is not otherwise exempt, will remain confidential and will only be disclosed to third parties with appropriate consent.

Where The Companies process personal data for direct marketing purposes either for its own benefit or under the instruction of clients, data subjects have the right to request an opt-out to these activities, which will be respected.

The Companies client direct marketing lists have been constructed using the double opt-in approach.

11. Sensitive Personal Data

The Companies do not process sensitive personal data as is defined in the GDPR. If this position changes, this Policy will be updated.

12. Rights of Access to Information

Data subjects (The Companies staff, clients, client's customers and prospective customers) have the right of access to information held by The Companies, subject to the provisions of the GDPR and the Freedom of Information Act 2000. Any data subject wishing to access their personal data should put their request in writing to The Companies.

The Companies will endeavour to respond to any such written requests as soon as is reasonably practicable and, in any event, within 40 days for access to records and 21 days to provide a reply to an access to information request. The information will be imparted to the data subject as soon as is reasonably possible after it has come to the attention of The Companies and in compliance with the regulation.

The Companies Managing Director is to be notified of all requests for information access.

13. Data Sharing

The Companies recognise that it is important that data entrusted to the business is only used for the purposes intended and that it is not shared beyond the consent received.

Where data relates to The Companies clients, data consents are captured in the contract with the client.

Where data relates to The Companies client customers or prospective customers, the individuals are informed at outset as to how their data will be used and whether it will be shared. Sharing of data would require consent.

Staff will notify the Managing Director of any data access request (where the data subject has requested access) for further review and consideration. No requests will be processed until the Managing Director has granted permission to proceed.

Where a contractually bound client requests the sharing of their customer or prospective customer data in the normal course of business, this request will be fulfilled without recourse to the Managing Director.

Any other form of data request should be referred to the Managing Director for review.

A log will be maintained of data sharing requests which fall outside of the normal business processing.

14. Data Transferability

The Companies support the ability of data subjects to move, copy or transfer their personal data from one IT environment to another in a safe and secure way, without hindrance to usability. The process to be employed to facilitate such requests would be assessed at the time to ensure they were appropriate and reasonable whilst maintaining compliance under the GDPR.

15. Automated Decision Making

The Companies do not undertake personal data automated decision-making including profiling.

16. Accuracy

The Companies will endeavour to ensure that all personal data held in relation to all data subjects is accurate. Data subjects must notify the data processor of any changes to information held about them. Data subjects have the right in some circumstances to request that inaccurate information about them is erased. This does not apply in all cases, for example, where records of mistakes or corrections are kept, or records which must be kept in the interests of all parties to which they apply.

Periodically, under the direction of or agreement from the clients of The Companies, client prospective customer marketing lists will be reviewed to ensure the data remains appropriate and up to date. This process may involve the client's prospective customer being contacted to ascertain whether they wish to remain on the lists, or to be deleted.

In addition, an annual Information Audit is undertaken to identify all sources of data, how and where the data is stored, used and deleted. This information audit is used to ensure that data held remains relevant, accurate and up to date.

17. Enforcement and Personal Data Breaches

If an individual believes that The Companies have not complied with this Policy or acted otherwise than in accordance with the GDPR, the member of The Companies staff aware of the grievance should raise the issue with the Managing Director. The grievance should also be notified to the ICO.

The grievance will then be monitored to a satisfactory conclusion by the Managing Director with any remedial actions and training being identified and implemented. Satisfactory closure includes closure of the grievance by the ICO.

18. Information Risk

The Companies manage information risk through the identification of areas of risk and the adoption of appropriate measures and processes to mitigate the risk. For example, the annual Information Audit is used to identify what data is stored, where, how it is used etc. One audit output is the identification of data flows from which information risk assessments are completed.

The Companies manage information risks in a structured way so that management understands the business impact of personal data related risks and manages them effectively, applying appropriate and reasonable mitigation processes.

Attention is also drawn to the existence of the *Information Security Policy and the Records Management Policy*, which provide more specific information on data protection processes and risk mitigation.

19. Data Protection Impact Assessment (DPIA)

The Companies will undertake DPIA's implementing appropriate and reasonable measures as a matter of its ongoing business and as developments occur, such as new clients, technology or processes.

20. Information Security

The Companies will take appropriate technical and organisational steps to ensure the security of personal data.

All staff will be made aware of this Policy and their duties under the GDPR.

The Companies and their staff are required to respect the personal data and privacy of others and must ensure that appropriate protection and security measures are taken against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to all personal data.

An appropriate level of data security must be deployed for the type of data and the data processing being performed. In most cases, personal data must be stored in appropriate systems.

Attention is also drawn to the existence of the *Information Security Policy and the Records Management Policy*, which provide more specific information on data protection processes.

21. External Processors

The Companies must take reasonable and appropriate steps to ensure that data processed by external processors, for example, service providers, Cloud services including storage, web sites etc. are compliant with this Policy and the relevant legislation.

22. Secure Destruction

When data held in accordance with this Policy is destroyed, it must be destroyed securely in accordance with best practice at the time of destruction.

Secure destruction of data will take place within the timescales agreed with The Companies client, acting as Data Controller under the GDPR, including contractual timescales, if this is appropriate.

The frequency of the secure destruction of data will depend upon it being an adhoc request from a client of The Companies, or during the Information Audit.

23. Data Processing Suppression Requests

The Companies clients, acting as Data Controllers under the GDPR, may request The Companies to suppress the processing of specific data at any point. The Companies will react to these requests as is reasonable and appropriate ensuring that the clients wish is met.

It is not in the commercial interests of The Companies to continue processing data which is not required by the client, nor would it be compliant with the GDPR.

24. Retention of Data

The Companies may retain data for differing periods of time for different purposes as required by clients, best practice or regulation.

The Companies may store some data indefinitely, such as client invoices and staff salary records.

25. CCTV

The Companies do not currently operate CCTV.