Data processing contract according to Art. 28 GDPR [EU General Data Protection Regulation]

The following data protection agreement is concluded between

Fabuglobal Limited/TA RangePrint
_____
Name
_____ 43 Plains Road, Mapperley
Address
_____ Nottingham, NG3 5JU

United Kingdom
_____

- hereinafter referred to as “Client" -

1. Subject matter and duration of the agreement

The order includes operational processing of personal data in connection with the provision of services.

Rangeprint processes personal data for the Client within the meaning of Art. 4 no. 2 and Art. 28 GDPR on the basis of this contract.

The contractually agreed service is provided exclusively in one of the member states of the European Union or in a contracting state of the Agreement on the European Economic Area. Any transfer of the service or parts of it to a third country shall require the prior consent of the Client and is allowed only if the special conditions of Art. 44 ff. of the GDPR are fulfilled (e.g., adequacy decision of the commission, standard data protection clauses, approved codes of conduct).

Duration of the contract:
The contract shall be concluded for an indefinite period of time. The Client can terminate the contract at any time without notice if a serious breach of data protection regulations or of the terms of this contract by Rangeprint exists, Rangeprint is unable or unwilling to comply with instructions of the Client, or if Rangeprint refuses the control rights of the Client in breach of the contract. In particular, noncompliance with the obligations stipulated in this contract and those derived from Art. 28 of the GDPR shall constitute a serious breach.

2. Purpose, scope and type of processing, nature of personal data and categories of data subjects

The processing of personal data on behalf of Rangeprint shall be carried out exclusively for the intended purpose.

The purpose of processing is processing and dispatch of print products as per the specifications of the Client, printed matter and printing requirements. These include, among others also the relevant invoicing and quality assurance.

Type of personal data:

- Employee data
- Data regarding interested parties/customers
- Communication data (e.g., relating to e-mail, internet, telephone)
- Contract master data
- Contract transaction data (for example, billing data and payment data)

Categories of affected persons:

- Last name, first name,
- Address
- Phone number
- E-mail address

3. Client's rights and obligations and its authority to issue directives

Rangeprint shall forward all such requests to the Client without delay, insofar as they are exclusively addressed to the Client in a recognisable manner. Rangeprint is not liable, if the request of the concerned person is not answered or not answered correctly or in time by the Client.

Changes to the subject matter of processing and procedural changes must be agreed between the Client and Rangeprint and specified in writing or in a documented electronic format.

The Client generally issues all orders, partial orders and instructions in writing or in a documented electronic format. Verbal instructions must be confirmed immediately in writing or in a documented electronic format.

The Client shall immediately notify Rangeprint, if he finds errors or irregularities while verifying order results.

The Client is obliged to treat confidentially all business secrets and data security measures of Rangeprint obtained within the scope of the contractual relationship. This obligation remains in effect even after termination of this contract.

4. Rights and obligations of Rangeprint

Rangeprint shall process personal data only within the framework of the agreements concluded and in accordance with the Client's instructions, unless it is obliged to do so by law of the Union or of the Member States to which the Client is subject (e.g., investigations by law enforcement or state protection authorities). In such a case, the Client shall inform Rangeprint of these legal requirements prior to processing, provided that the law in question does not prohibit such notification on the grounds of an important public interest.

Rangeprint shall not use the personal data provided for processing for any other purposes, in particular, not for its own purposes. Copies or duplicates of personal data shall not be prepared without the

knowledge of the Client. Exceptions are technically essential duplications, provided the level of data protection agreed here is not compromised.

Rangeprint assures that all agreed measures will be contractually implemented in relation to the commissioned processing of personal data. Rangeprint assures that the data processed for the Client will be kept strictly separate from other data inventories.

Rangeprint will support the Client to the extent possible in fulfilling the inquiries and demands of concerned persons as per chapter III of the GDPR and complying with the obligations mentioned in Art. 33 to 36 GDPR.

Rangeprint shall promptly notify the Client, if it is of the opinion that any of the instructions issued by the latter are in breach of statutory regulations. Rangeprint is entitled to suspend the implementation of the relevant instruction until such time as it is confirmed or modified after review by the person responsible on behalf of the Client.

Rangeprint shall correct, delete or restrict the processing of personal data from the contractual basis, if the Client requests this by means of an instruction and if this does not conflict with legitimate interests of Rangeprint.

Rangeprint is allowed to provide information about personal data from the contractual basis to third parties or the parties concerned only after prior instruction or approval by the Client.

Rangeprint agrees that the Client is - by appointment - entitled to monitor compliance with the provisions on data protection and data security, as well as the contractual agreements to an appropriate and necessary extent either on its own or via third parties commissioned by the Client, in particular, by obtaining information and inspecting the stored data and data processing programs, as well as by means of on-site checks and inspections.

Rangeprint assures that it shall assist in these checks where necessary. Checks shall be carried out during normal business hours without disruption to operations after notification, taking into account an appropriate lead time. If Rangeprint provides evidence of the correct implementation of the agreed data protection obligations as stipulated in Annex 2 to this Agreement, control shall be limited to spot checks.

Rangeprint is allowed to make the controls subject to prior notification with a reasonable lead time and to the signing of a non-disclosure agreement regarding the data of other customers and the technical and organisational measures set up. If the inspector commissioned by the Client is in a competitive relationship with Rangeprint, Rangeprint has a right to object to this.
If a data protection supervisory authority or any other sovereign supervisory authority of the Client carries out an inspection, the above paragraph shall apply mutatis mutandis. It is not necessary to sign a confidentiality agreement if the supervisory authority is subject to professional or legal secrecy, in which a violation is punishable under the Criminal Code.

Insofar as Rangeprint incurs costs in terms of time or financial expenses to enable controls by the customer, it may demand an appropriate remuneration for this.

Rangeprint confirms that it is aware of the relevant data protection regulations of the GDPR applicable to order processing.

Rangeprint undertakes to maintain confidentiality when processing the Client’s personal data in accordance with the contract. This shall continue to exist even after termination of the contract.

Rangeprint assures, that prior to commencing work, it will familiarise the employees deployed to carry out the work with the provisions of data protection which are relevant for them and that it will be oblige them to maintain confidentiality in an appropriate manner for the duration of their work and also after termination of the employment relationship. Rangeprint shall monitor compliance with data protection regulations in its company.

Rangeprint will notify a change of the data protection officer within a reasonable period of time.

5. Rangeprint notification obligations in the event of processing disruptions and violations of the protection of personal data

Rangeprint shall immediately notify the Client of any disruptions, infringements by Rangeprint or its employees of data protection regulations or the provisions set out in the contract, and suspicion of data protection violations or irregularities in the processing of personal data. This also applies, in particular, with regard to possible notification and information obligations of the Client as per Art. 33 and Art. 34 GDPR. Rangeprint undertakes to provide the Client with appropriate support to fulfil his obligations under Art. 33 and 34 of GDPR. Notifications according to Art. 33 or 34 DS-GMO for the Client can only be issued by Rangeprint after prior consultation with the Client.

6. Subcontracting relationships with subcontractors for core services

The Client hereby agrees that Rangeprint may commission subcontractors in the course of service provision; subcontractors can also be companies affiliated with Rangeprint.

Subcontractors may be engaged in third countries only if the special requirements of Art. 44 ff. GDPR are fulfilled (e.g., adequacy decision of the commission, standard data protection clauses, approved codes of conduct).
The contract with the subcontractor must be made in writing, it can also be done in an electronic format.

Rangeprint will ensure that the contract with the subcontractor imposes at least the same obligations on him, as imposed on Rangeprint under this contract.

A list of the subcontractors deployed by Rangeprint at the start of contract can be found in Annex 1. Rangeprint will inform the customer of any new subcontractor before the same accesses any personal data. The Client may object in writing to the commissioning of a new subcontractor for important reasons within ten (10) days after receipt of the notification if the subcontractor does not meet the requirements of this agreement and those of this data protection agreement and the service contract. The failure of the Client to object within this period shall be deemed to constitute consent to the commissioning of the new subcontractor. The Client is aware that not engaging a new subcontractor can lead to a delay, or non-performance of the service and increased prices. Rangeprint shall inform the Client of any degradation of performance or increase in prices resulting from the Client's objection to engaging a new subcontractor. The Client can then either demand a supplement to the service contract in order to take into account the changes, or terminate the service contract as per the provisions provided therein. Such termination shall not constitute a termination for good cause or for breach of contract.

Rangeprint shall be responsible and liable for the acts, omissions, poor performance or non-performance of its subcontractors to the same extent as under its own performance obligations under this Agreement.

7. Technical and organisational measures according to Art. 32 GDPR

Rangeprint has to establish security as per Art.28 para 3 lit. c, Art 32 GDPR particularly in connection with Art. 5 para 1, para 2 GDPR. Overall, the measures to be taken are measures of data security and measures to ensure an appropriate level of protection corresponding to the risk with regard to the confidentiality, integrity, availability and resilience of the systems In doing so the state of the art, the cost of implementation and the type, the scope and the purpose of processing as well as the different probability of occurrence and the severity of the risks to the rights and freedoms of the natural persons concerned within the meaning of Art. 32 para. 1 GDPR must be taken into account.

The data protection concept described in Annex 2 sets out the minimum requirements of the technical and organisational measures suitable for the risk to be determined, taking into account the protection objectives according to the state of the art and taking particular account of the IT systems deployed and processing steps used at Rangeprint.

The measures taken at Rangeprint can be adapted to technical and organisational developments during the course of the contractual relationship, but must not fall below the agreed standards.

Rangeprint regularly monitors internal processes and technical and organizational measures to ensure that processing within its area of responsibility is carried out in accordance with the requirements of applicable data protection law and that the rights of the data subjects are protected.

If an inspection or an audit by the client shows that there is a need for adjustment, this must be implemented by mutual agreement. If the Client's requirements go beyond the level of protection that Rangeprint had accepted initially, and these are not requirements that Rangeprint has to implement for all other contracting entities anyway, then can demand an appropriate remuneration from the Client for the implementation.

8. Obligations of Rangeprint after completion of the order

Upon completion of the Contractual Work, Rangeprint shall return to the client all data, documents and processing and utilisation results obtained in connection with the contractual relationship still in its possession and in the possession of the subcontractors. Alternatively, with prior consent, delete and destroy them in accordance to Data Protection Regulations.

However, this only applies if no legal retention periods for the data have to be observed by Rangeprint.

The Protocol of deletion or destruction shall be confirmed by the client on request

Documentation serving as proof of a proper standard of data processing in line with the contractual agreement during the term of the contractual service, shall be retained by Rangeprint beyond the end of the agreement in accordance with the relevant retention periods. Rangeprint may however, hand over the documentation to the client at the end of the contract for its own exoneration.

9. Liability

The Liability of the parties under this agreement is limited in the same manner as in the relevant contractual service agreement.

10. Misc

Side agreements shall require the written form or a documented electronic format

The place of Jurisdiction for Rangeprint is the local court of Jurisdiction

Should individual provisions of this agreement be or become invalid or void, this shall not affect the validity of the contact. The unenforceable provision shall be substituted for a suitable provision that most closely fulfils the intentions of the agreement.

Annex 1 - Subcontracting relationships

The following subcontracting relationships currently exist in connection with order processing:

Company subcontractor	Address
Minuteman Press Nottingham	43 Plains Road Mapperley, Nottingham, NG3 5JU
Fabuglobal Limited	43 Plains Road Mapperley, Nottingham, NG3 5JU

Annex 2 - Technical and organisational measures/data protection concept

Rangeprint assures that it will comply with the minimum requirements described below within the framework of its data protection concept. It describes the measures required at Rangeprint in the course of order processing, necessary to ensure secure handling of personal data. The basis for this data protection concept is the EU General Data Protection Regulation (GDPR) and, if necessary, other measures required by the parties. In this context, Rangeprint will essentially follow the provisions of Articles 24, 25 and 32 of the GDPR.

Upon request, Rangeprint shall provide evidence of compliance.

1. Confidentiality

1.1. Entry controls

The rooms in which the processing of personal data is carried out or in which data processing systems are installed shall not be freely accessible. They must be locked when the employee is absent. The access authorisations must be issued in a regulated procedure according to the "need to know principle" and must be monitored regularly with regard to their necessity. Rooms in which data processing systems (data centre, servers, network distributors, etc.) are housed must be particularly access controlled and may be accessible only to the employees of the IT administration (if required, the management). Alternatively, the devices must be stored in suitable and locked cabinets. Visitors and persons outside the company must be registered in a documented procedure and supervised within the premises.

1.2. Access control

For every network user there has to be a personally allocated user password with a password consisting of at least 4 characters with upper case and lower-case letters. Users must be obliged by the system to change their passwords at least every 180 days. Network users shall be required to document compliance with the user access policy. The provision, modification and withdrawal of access rights must be carried out in a documented procedure. Configured access authorisations must be regularly checked and documented for their necessity. Network access must be monitored and logged, including unsuccessful logon attempts. A network access must be automatically blocked by the system after 3 unsuccessful attempts at the latest.

1.3. System access controls

In order to access personal data, a documented, role-based authorisation concept must be in place that restricts access to the data so that only authorised persons can access the personal data necessary for their task (minimum principle). The password regulations from access control must also be implemented as part of access control. Administrative activities must be restricted to a small group of administrators. The activities of the administrators must be monitored and logged within the framework of technically justifiable expenditure.

1.4. Pseudonymisation

Assessments must be pseudonymised if the personal reference to the result is not absolutely necessary.

1.5. Segregation control

Separation of personal data must be ensured by different storage locations or by client separation.

2. Integrity

2.1. Data relay control

As part of transfer control, it must be ensured that only authorised persons can take note of the personal data. Mobile devices or mobile storage media must be encrypted if personal data is stored on them.

2.2. Data entry controls

It must be possible to assign the entry, modification and deletion of personal data to the performing employee. Changing and deletion of data records must be restricted by the system to effectively prevent accidental changes or deletions.

2.3. Contract control

As part of the contract control, it must be ensured that the data processing operations carried out on behalf of Rangeprint in the context of an order are carried out exclusively upon the instruction of Rangeprint. For this purpose, the employees involved in data processing must be trained and instructed. Order processing must be monitored by internal controls. The results of the controls must be documented.

Subcontractors may be engaged only on the basis of the regulations agreed with the Client. The transfer or access to personal data may not take place until the subcontractor has signed an agreement on order processing in accordance with Art. 28 of the GDPR and has confirmed compliance with the regulations of the data protection concept. The Contractor's obligation to check its subcontractor results from the order processing agreement concluded with the Client.

3. Availability and resilience

Personal data must be processed on data processing systems that are subject to regular and documented patch management. Security-relevant patches must be applied after announcement. The continuous availability of personal data must be guaranteed by means of redundant storage media and data backups in accordance with the state of the art. Servers must have an uninterrupted power supply (UPS) that ensures controlled shut-down without loss of data.

4. Periodic review, assessment and evaluation procedures

A procedure for monitoring data protection in the company must be implemented. This must include the obligation of employees to maintain data secrecy, training and sensitisation of employees, and regular auditing of data processing procedures. Similarly, the documentation of the processing procedure performed for Rangeprint must be completed before data processing is commenced. For data protection

violations and the protection of the rights of those affected, a continuous reporting and processing process must be introduced. This must also include information from Rangeprint.