

EU GENERAL DATA PROTECTION REGULATION – DATA PROCESSING REQUIREMENTS

PROCESSOR NOTIFICATION

The EU General Data Protection Regulation (“**GDPR**”) will apply from 25 May 2018 and will fully replace existing national data protection legislation (i.e. the UK Data Protection Act 1998). Whilst certain existing provisions will remain the same, the GDPR also introduces new and additional data protection obligations on companies handling personal data, data controllers and data processors.

The GDPR imposes specific obligations on Controllers and Processors of Personal Data. The GDPR requires Controllers and Processors to enter into contracts containing specific provisions relating to the protection of the Personal Data processed. A significant change introduced by the GDPR is the requirement to ensure that contracts with “data processors” include certain minimum terms.

You have received this letter because:

- a) We have entered into one or more agreements in respect of the provision of services by emPSN Limited (“emPSN”) to you; and
- b) emPSN believes that in providing such services to you under the Order Forms and terms and condition of services, we may collect and process your Personal Data as a Processor.

In light of this emPSN are writing to notify you that, with effect from 25th May 2018, emPSN will Process your Personal Data in accordance with our obligations under Article 28 GDPR as set out below:

For the purposes of this letter the capitalised terms shall have the following meanings:

“**emPSN**” means the legal entity identified and named at the end of this letter;

“**Data Protection Laws**” means any applicable law relating to the processing, privacy and use of Personal Data, as applicable to either party or to the Services including:

- (a) the Directive 95/46/EC (Data Protection Directive) and/or Data Protection Act 1998 or the GDPR;
- (b) any laws which implement any such laws;
- (c) any laws that replace, extend, re-enact, consolidate or amend any of the foregoing; and
- (d) all guidance, guidelines, codes of practice and codes of conduct issued by any relevant Supervisory Authority relating to such Data Protection Laws (in each case whether or not legally binding);

“**Data Subjects**” has the meaning given in applicable Data Protection Laws from time to time;

“**International Organisation**” has the meaning given in applicable Data Protection Laws from time to time;

“**Member State**” means any relevant member state of the European Union (“**EU**”) or European Economic Area (“**EEA**”) from time to time;

“Personal Data” has the meaning given in applicable Data Protection Laws from time to time;

“Processing” has the meaning given in applicable Data Protection Laws from time to time (and related expressions, including “process”, “processed” and “processes” shall be construed accordingly);

“Services” means those services referred to in the Service Agreements;

“Sub-Processor” means any operator who provides to emPSN products or services; (ii) agent; (ii) subcontractor; or (iii) other third party; engaged by emPSN who carries out any Processing activities in respect of the Personal Data;

“Supervisory Authority” means any regulator, authority or body responsible for administering Data Protection Laws.

emPSN shall:

1. Process your Personal Data for the sole purpose of providing the Services and in accordance with your written instructions or as is required by law or any Supervisory Authority.
2. Process the Personal Data only on documented instructions from you, including with regard to transfers of Personal Data in or to countries outside the EEA or to any International Organisation with your prior written consent, unless required otherwise to comply with any EEA or Member State law (in which case, you shall provide prior notice to emPSN of such legal requirement, unless that law prohibits this disclosure on important grounds of public interest).
3. obtain a commitment of confidentiality from anyone it allows to process the Personal Data, unless they are already under such a duty by law.
4. implement and maintain (or if at your premises use your systems and comply with your) appropriate technical and organisational measures against unauthorised or unlawful Processing of, and against accidental loss or destruction of, or damage to, your Personal Data.
5. in relation to the Processing of Personal Data and taking into account the nature of the Processing, assist you insofar as is possible in the fulfilment of your obligations to respond to Data Subject requests relating to Personal Data.
6. assist you in ensuring compliance with the obligations pursuant to Articles 32 to 36 GDPR, taking into account the nature of Processing and the information available to emPSN.
7. not (unless otherwise permitted in accordance with the terms of the Service Agreements) engage a Sub-Processor for carrying out any Processing activities in respect of the Personal Data without your written authorisation of that specific Sub-Processor (such authorisation not to be unreasonably withheld, conditioned or delayed). emPSN shall inform the Customer of any intended changes concerning the addition or replacement of other processors, thereby giving the Customer the opportunity to object to such changes. emPSN shall appoint such Sub-Processor under a written contract containing materially the same obligations as set out in this letter.

8. record and refer all requests and communications received from Data Subjects or any Supervisory Authority to you which relate (or which may relate) to any Personal Data promptly and shall not respond to any without your express written approval and strictly in accordance with your instructions unless and to the extent required by law.
9. provide such information and assistance (including by taking all appropriate technical and organisational measures), insofar as this is possible, to assist you in the fulfilment of your obligations to respond to requests for exercising the Data Subjects' rights under Chapter III of the GDPR (and any similar obligations under applicable Data Protection Laws).
10. provide such information, co-operation and other assistance (taking into account the nature of Processing and the information available to emPSN) to assist you in your obligations under Data Protection Laws, including with respect to:
 - security of Processing;
 - assistance to notify Personal Data breaches to the relevant Supervisory Authority;
 - assistance to advise Data Subjects when there has been a Personal Data breach;
 - data protection impact assessments (as defined in the Data Protection Laws); and
 - consulting with the relevant Supervisory Authority regarding high risk Processing.
11. (and ensure that any Sub-Processors shall) without delay, at your written request, either securely delete or securely return all the Personal Data to you in such form as you reasonably request after the earlier of:
 - the end of the provision of the relevant Services related to Processing of such Personal Data;
 - or
 - once Processing by emPSN of any Personal Data is no longer required for the purpose of emPSN' performance of its relevant obligations under the Service Agreements;and securely delete existing copies (except to the extent that storage of any such data is required by applicable law).
12. (and shall ensure any Sub-Processors shall) promptly make available to you such information as is reasonably required to demonstrate emPSN' and your compliance with our respective obligations under this letter and the Data Protection Laws, and allow for, permit and contribute to audits, including inspections, by you (or another auditor mandated by you) for this purpose at your request from time to time. emPSN shall provide (or procure) access to all relevant premises, systems, personnel and records during normal business hours (09:00 – 17:00) for the purposes of each such audit or inspection upon reasonable prior notice (not being more than two Business Days) and provide and procure all further reasonable co-operation, access and assistance in relation to any such audit or inspection.

The terms of this letter clearly defines emPSN's obligations which will be incorporated into and form and integral part of the legal basis of our relationship with you.

Please note that the requirements set out herein have been limited to what is required by the GDPR. As a result, we regard these provisions as non-negotiable and part of a business operating in accordance with the new Data Protection Law.

Should you have any queries or concerns in respect of the terms of this letter, please email empsn@empsn.org.uk.