GDPR – Data Controller / Processor Contract

Data Controller / Processer Contract

As a result of activities the gas-*elec* Group* carry out on your behalf, we may need to hold and process personal data.

(*Gas-elec Safety (UK) Ltd, Gas-elec Bureau (UK) Ltd (GBS), Gas-elec Holdings Ltd, Safety Choice Ltd and gas-*elec* franchise network)

The legal basis on which we hold the data is that it is necessary to carry out contracted services. No marketing of unrelated products and services will be undertaken using this data unless specific consent has been obtained from the data subject.

In the course of processing, purely in pursuance of the contracted task, and subject to GDPR compliant contracts, gas-*elec* may transfers personal data to the following organisations - Barclays Bank for payment processing, UK Fast who host our servers, Webfusion who provide our email & server to host the email, Google inc. online storage. gas-*elec* will provide details of engineering contractors carrying out services on its behalf, upon request.

gas-*elec* has updated its terms and condition take account of changes in data protection regulations. All data will now be collected, stored and processed subject to these new conditions.

Relevant legislation is;

The Data Protection Act 1998 and the Privacy and Electronic Communications (EC Directive) Regulations 2003 and, from 25 May 2018, The General Data Protection Regulation, including legislation implemented in connection with the regulation.

General Data Protection Regulation (GDPR) refers to Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data.

The legislation distinguishes between Data Controllers, who determine the purpose for which, and manner in which personal data is processed. Data Processors carry out processing on behalf of the Data Controller.

For example, if we are carrying out services for private landlords, we would be controllers with respect to the landlord's data, which we would use for order processing, but data processors for the tenant data which we would use to arrange access on the landlord's behalf. Carrying out the same service on instruction from a letting agent, the agent would be the controller for the landlord's data as well as the tenant data.

The obligations and rights of the controller

Data quality principles – The controller must comply with the "data quality principles".

- Legal basis for processing – Personal data can only be processed where the controller has a legal basis for that processing.
- Data Security – Controllers must implement appropriate technical and organizational security measures to protect personal data.
- Data protection "by design" and "by default – Controllers must ensure that, in the planning phase of processing activities and implementation phase of any new product or service, data protection principles and appropriate safeguards are addressed/ implemented.
- Joint controllers – Where two or more Controllers act together they are "Joint Controllers" and must, by means of an "arrangement" between them, apportion data protection compliance responsibilities.
- Liability of Joint Controllers – Joint Controllers are jointly and severally liable. A Joint Controller may be exempt from liability if it proves that it is in no way responsible for the damage. If it pays full compensation to the affected data subjects, then it may bring proceedings against other Joint Controller(s) to recover that compensation.
- Records of Processing Activities - Controllers must keep records of their processing activities. Upon request, these records must be disclosed to DPAs.
- Appointment of Processors – A Controller must only appoint a Processor under a binding written agreement, which states that the Processor must:
    i. Only act on the Controller's documented instructions;
    ii. Impose confidentiality obligations on all personnel who process the relevant data;
    iii. Ensure the security of the personal data that it processes;
    iv. Abide by the rules regarding appointment of sub-processors;
    v. Implement measures to assist the Controller in complying with the rights of data subjects;
    vi. Assist the Controller in obtaining approval from DPAs where required;
    vii. At the Controller's request, either return or destroy the personal data at the end of the relationship; and provide the Controller with all information necessary to demonstrate compliance with the GDPR.
- Reporting data breaches to DPAs – Controllers must report a data breach to the relevant DPA within 72 hours of their becoming aware of that breach, except where the data breach is unlikely to result in any harm to data subjects.
- Notifying data breaches to affected data subjects – Where a data breach causes a high degree of risk to data subjects, Controllers must notify the affected data subjects without undue delay.
- Compliance obligations under the GDPR (Rec. 22; Art. 3(1)) – The GDPR imposes legal compliance obligations directly on Processors (in addition to Controllers).
- The Processor must comply with the Controller's instructions (Art. 28(10)) – Where a Processor determines the purposes and means of any processing activity, that Processor is treated as a Controller in respect of that processing activity.
- Records of processing activities (Rec. 82; Art. 30(2)) – Each Processor (and any of its representatives) must keep records of its processing activities performed on behalf of the Controller (which include certain prescribed information).
- Cooperation with DPAs (Art. 31) – Processors (and any of their representatives) are required to cooperate, on request, with DPAs in the performance of their tasks.
- Obligation to appoint a DPO (Art. 37) – To the extent that the GDPR requires the appointment of a Data Protection Officer (a "DPO"), that requirement applies to Processors as well.
- Restrictions on Cross-Border Data Transfers (Art. 44) – The obligation to ensure that there is a lawful basis for all Cross-Border Data Transfers applies directly to Processors as well as controllers.
- Liability of Processors (Rec. 146; Art. 82(1)-(2)) – Data subjects can bring claims directly against a Processor (but only where it has not complied with its obligations under the GDPR or acted outside/contrary to lawful instructions of the Controller).

Obligations of the Data Processor

- The Data Processor must only act on the written instructions of Data Controller (unless required by law to act without such instructions);
- The Data Processor must ensure that people processing the data are subject to a duty of confidence;
- The Data Processor must take appropriate measures to ensure the security of processing;
- The Data Processor must only engage a sub-processor with the prior consent of Data Controller and a written contract;
- The Data Processor must assist Data Controller in providing subject access and allowing data subjects to exercise their rights under the GDPR;
- The Data Processor must assist Data Controller in meeting its GDPR obligations in relation to the security of processing, the notification of personal data breaches and data protection impact assessments;
- The Data Processor must delete or return all personal data to Data Controller as requested at the end of the contract.
- The Data Processor must submit to audits and inspections, provide Data Controller with whatever information it needs to ensure that they are both meeting their Article 28 obligations, and tell Data Controller immediately if The Data Processor are asked to do something infringing the GDPR or other data protection law of the EU or a member state.
- Nothing within the contract relieves The Data Processor of its own direct responsibilities and liabilities under the GDPR;
- In addition to the Article 28.3 contractual obligations set out in the controller and processor contracts checklist, a processor has the following direct responsibilities under the GDPR. The Data Processor must:
    - Only act on the written instructions of Data Controller (Article 29);
    - Do not use a sub-processor without the prior written authorisation of Data Controller (Article 28.2);
    - Co-operate with supervisory authorities (such as the ICO) in accordance with Article 31;
    - Ensure the security of its processing in accordance with Article 32;
    - Keep records of its processing activities in accordance with Article 30.2;
    - Notify any personal data breaches to Data Controller in accordance with Article 33;
    - Employ a data protection officer if required in accordance with Article 37; and
    - Appoint (in writing) a representative within the European Union if required in accordance with Article 27.
    - A processor should also be aware that:
        - it may be subject to investigative and corrective powers of supervisory authorities (such as the ICO) under Article 58 of the GDPR;
        - if it fails to meet its obligations, it may be subject to an administrative fine under Article 83 of the GDPR;
        - if it fails to meet its GDPR obligations it may be subject to a penalty
        - under Article 84 of the GDPR; and
        - if it fails to meet its GDPR obligations it may have to pay compensation under Article 82 of the GDPR.

Data for which we are Data Controllers

Categories of Data subject;	Letting Agents, Homeowners, Landlords
Data type;	Name, address, telephone number, email address, bank card details
Nature of processing;	Communication regarding contract, invoicing and certificate delivery.
Duration;	Bank details are not stored but passed directly to Barclays Bank in exchange for a single use token to be redeemed on completion of work. Contact details are retained for warranty period of product purchased or until expiry of safety certification, whichever is the longer.

Data for which we are Data Processors

Categories of Data Subject;	Landlords, tenants.
Data type;	Name, address, telephone number, email address, bank card details
Nature of processing;	Communication regarding contract, invoicing and certificate delivery. Tenant's details are used in arranging access to carry out safety inspections or other work, and for delivery of safety certificates.
Duration;	Bank details are not stored but passed directly to Barclays Bank in exchange for a single use token to be redeemed on completion of work. Contact details are retained for warranty period of product purchased or until expiry of safety certification, whichever is the longer. Tenant's data will be deleted once access for the contracted works is completed unless recorded as part of a safety certificate where statutory minimum retention periods apply.

As a part of GDPR, use of Data Processors by Data Controllers must be covered by contracts. In contracting services from gas-*elec*, in the absence of a specific data processing / controlling agreement(s) with yourselves, you agree to be bound by the above terms.