

Aga Rangemaster Group (“ARG”) Policy on Compliance to Data Protection Legislation and the privacy of individual data General Policy Statement (“Policy”)

Chapter 1 – Purpose of the policy

The purpose of this policy is three-fold:

- To ensure that ARG complies with the prevailing privacy and data protection legislation in the countries in which it operates.
- To ensure that ARG businesses adopt best-practice with regard to the use and privacy of individual data in accordance with the principles set out by organisations such as the Direct Marketing Association in the UK.
- To ensure that we meet the expectations of our customers, employees and any other individuals with whom we have contact, with regard to the way we process and store data concerning individuals.

The specific requirements with regard to ARG's employee data and individual access rights are covered by a separate HR policy (this is appended). Consequently, data handling practices related to personnel management (payroll, employee records, CCTV policy) are not specifically addressed by this policy, but the general principles set forth in this policy will govern implementation of the HR policy.

To which business units does this policy apply:

This policy applies to any business unit which processes personal data, i.e. stores or uses personal data. This means that every business unit is affected because the definitions of “processing” and “personal data” are both very wide. For instance, "**personal data**" includes the following (non-exhaustive) types of data:

- Employee details
- Customer i.e. consumer data, including name, address, and financial information
- Customer contact data of business or trade customers
- Supplier contact data

"**Processing**" captures almost any data handling activity, including sorting personal data or entering it onto a computer.

To be compliant with the relevant data protection legislation, each business unit must abide by the terms of this policy, with the "Eight Principles of Good Practice" (set out below) and must be notified with to the appropriate data protection authority (the Information Commissioner in the UK) that it processes personal data. There are severe financial penalties for non-compliance

Chapter 2 – Scope and principles of the policy

This policy is largely based on the data protection legislation in force in the UK, which implements the EU Data Protection Directive. There will be variations in certain countries based on differing applications of the Directive and it is the responsibility of each non-UK business unit to take account of these differences in their day-to-day operations. However, conformance to the general principles below will cover most legal obligations and is a basic, mandatory requirement for all units:

There are **Eight Principles of Good Practice** as set out in the UK Data Protection Act 1998 ("DPA"), which require that data must be:

1. Fairly and lawfully processed;
2. Processed for limited purposes;
3. Adequate, relevant and not excessive (i.e. the data's quality);
4. Accurate and up-to-date;
5. Not kept longer than necessary (i.e. retention periods);
6. Processed in accordance with the individual's rights (their "Data subject Access Rights");
7. Kept secure and confidential;
8. Must not be transferred to countries outside the European Economic Area (EEA) unless the receiving country has adequate protection for the individual (third country transfers).

At least one of the six following conditions must be met for personal data to be considered fairly processed:

- a) the individual has consented to the processing;
- b) processing is necessary for the performance of a contract with the individual (e.g. to make a delivery of a product);
- c) processing is required under a legal obligation (other than one imposed by the contract);
- d) processing is necessary to protect the vital interests individual;
- e) processing is necessary in order to carry out public functions (e.g. the administration of justice); and/or
- f) processing is necessary in order to pursue the legitimate interests of the data controller or third parties (unless it could unjustifiably prejudice the interests of the individual).

It should be noted that there are specific rules that apply to processing "**Sensitive Personal Data**" about individuals. Sensitive personal data includes information about racial or ethnic origin, political opinions, religious or other beliefs, trade union membership, physical or mental health condition, sex life, criminal proceedings or convictions. Such data can only be processed if the explicit consent of the individual is given OR if it is required by law to process such information for employment purposes, OR if this information needs to be processed to protect the vital interests of the individual or another person, OR if required for the administration of justice/legal proceedings.

Outside the HR context there should be few occasions where it will be necessary to collect sensitive personal data from an individual and such occasions should be kept to a minimum.

Chapter 3 – Implications for Aqa Rangemaster Group plc under the Data Protection Act

The following Policy must be followed by all UK units of the Aqa Rangemaster Group plc:

1. All UK business units must either be notified with the Information Commissioner in their own right, or must be listed under the notification of one of the Aqa Consumer Products limited companies' notifications e.g. Aqa Consumer Products Limited. These registrations also need to be renewed annually. Similar notifications will be required in other EEA countries. (See the Public Register at www.informationcommissioner.gov.uk).
2. The following policy guidelines must be followed by all business units in order to conform to the requirements of the DPA:
 - a. Business units must only collect the amount of personal data needed to satisfy the contract with the customer (e.g. delivery address/telephone number etc).
 - b. If a business unit asks for more personal data e.g. email address then they must make the customer aware that this is being done for use in further direct marketing and appropriate consents should be obtained (see below).
 - c. Because of the stringent rules regarding transferring personal data to third parties, and because we would need to ask permission in all cases when collecting personal data, business units should not transfer any personal data to third parties for marketing purposes. The only acceptable exception to this are mailing houses and in this case a third party processing agreement must be signed by both the Aqa unit and the third party (see example attached).
 - d. Individuals must be given the option of opting out from receiving further contact from us, i.e. they must be given the opportunity to opt-out on every occasion they are mailed, emailed or telemarketed and their wishes must be recorded centrally and honoured.
 - e. Every contact with an individual or customer must follow these rules and ALL forms through which we collect personal data (questionnaires, order forms, home delivery forms, websites and online registration systems, etc.) should set out the uses to which the data collected will be put. These forms should also be used to obtain the appropriate consents for processing, when necessary.

- f. Business units must note that the data they collect may be used by other business units in the Aga Rangemaster Group and so we all have a collective responsibility to process personal data in the correct way and to always give the opportunity for the individual to opt-out from contact with the Aga Rangemaster Group as a whole.
- g. Any telemarketing, email or mail out activity should only be directed at individuals who have not opted out and must include a mechanism for opting out in the future (e.g. a tick box on a mail reply paid card). If telemarketing is performed on a bought-in list then the first contact with the customer must include an easy means of opting out e.g. "unsubscribe". This is also true for email marketing activities.
- h. All arrangements for third party processing must be the subject of a signed data processing agreement. This includes third party processing for e.g. payroll processing, mailing houses, companies from whom we buy mailing lists, delivery companies, third parties who host servers for the group and generally any third party who has access to individual personal data which we may have collected/are processing. Such agreements must include clauses to the effect that the third party conforms with the relevant data protection legislation and will continue to be compliant, and specific requirements include but are not limited to:
 - i. Adequate assurance as to the security of data in terms of both backups and security of access.
 - ii. Explicit identification of which party is the data controller (party responsible for determining what will be done to the data, and hence legally responsible under the DPA) and which party is the data processor (party carrying out the data controller's instructions vis-à-vis the data).
 - iii. Assurances that any personal data provided to the Aga Rangemaster Group plc has been obtained with the appropriate consents from the individuals concerned.
 - iv. Assurances that any information which we pass on to them will only be processed according to our instructions and will not be used by them for any other purpose or activity e.g. their own direct marketing, and information will not be divulged to any third party.
- i. Because the quality and integrity of personal data is covered by the DPA, all personal data that we collect must have the following applied to it:
 - i. Regular review and de-duplication.
 - ii. Data must be current. Therefore, any customers that have not been contacted in a two year period - and thereby given the ability to opt-out should be deleted from all marketing databases and printed copies thereof, and in no circumstances should they be contacted.
 - iii. Before contacting customers by direct mail or fax, data should be checked against "The Bereavement Register" (TBR), "Gone Away Suppression" (GAS) and "Mailing Preferences" (MPS)

/Fax Preferences (as appropriate). Checks against these registers are typically done by the mailing house or other organisation “cleansing” the data and there is normally a charge for each “match” detected. (See the Direct Marketing Association’s guidelines at www.dma.org.uk for further information).

- iv. Individuals contacted by mail or fax should have the opportunity to opt-out and these should be recorded and honoured.
- v. Individuals contacted by email should have the opportunity to “unsubscribe” and these should be recorded and honoured.
- j. Because under the DPA data must be kept secure and confidential, the following must apply to all personal data (this includes employees, customers, supplier contacts, subcontractor contacts, etc):
 - i. Paper-based data must be kept secure in locked filing cabinets.
 - ii. Electronic data must be regularly backed up and subject to password access to authorised users only. Computers, software and data storage should be properly secured when not in use.
 - iii. Employees must understand their responsibility for any data to which they have access and their obligation not to disclose any personal data which they come across in the course of their job.
 - iv. Where “lists” are bought-in, individuals on those lists must be given the option to opt-out from further communications by mailing them as soon as possible. Any opt-outs should be recorded centrally and honoured.
 - v. Waste paper and printouts containing personal data should be shredded or disposed of as confidential waste.
- k. All business unit websites must have a privacy statement which includes the following:
 - i. A statement to the effect that information will not be passed to third parties without the relevant individual's consent.
 - ii. A statement to the effect that individual data may be used for direct marketing by the unit/by other Aga Rangemaster Group companies and the individual should be given the opportunity to opt-out from this use of their data.
 - iii. Where information gathering devices such as cookies are used then this must be disclosed along with the purpose for which they are used and provide an option for the individual not to accept the cookies.
- l. Each business unit of the Aga Rangemaster Group will appoint a Data Protection Compliance Officer and any individual wishing to exercise their right to access their personal data, as permitted by the DPA will

contact the Compliance Officer. The Compliance Officer will need to be fully trained in ARG's policies (this one and the HR policy), the Eight Principles of the DPA and in the process by which individuals can apply for access to their data. The Group Data Protection Compliance Officer is Pam Sissons, Aga Rangemaster Group plc, 4 Arleston Way, Shirley, Solihull, B90 4LH. Tel. 0121 711 6000, Fax 0121 711 6001, e-mail secretarial@agarangemaster.com.

- m. Each business unit must train its employees in the Eight Principles of the DPA, their responsibilities under this policy including, but not limited to, collecting the appropriate level of consent from customers, etc., and non-disclosure of personal data.
- n. The use of CCTV footage will in general only be used for the prevention of crime and giving assistance to enforcing authorities i.e. the police. The fact that CCTV is in use must be notified to employees and other persons by way of notices. If CCTV is used for any other purpose, e.g. monitoring staff, then this fact must be notified via the notices. Regular checks must be made to ensure that cameras are working correctly. Please consult the HR Policy for more information on ARG's CCTV policy.
- o. There are special provisions in the DPA with regard to responsibilities when transferring data concerning individuals to countries outside of the EEA. The policy in this area is that such data will not be transferred out of the EEA unless the business unit has evidence that the information originates outside of the EEA and data is being forwarded at the individual's specific request e.g. a consumer in Australia who has asked for details of their local dealer.
- p. Because the individual has the right to request access to data held about him or her (in whatever form) and because this may be an employee, customer or customer/supplier contact, then care should be taken when recording such information and the data collected should be appropriate to the purpose for which it is collected.
- q. Each unit shall develop an internal process for responding to individual access requests within the prescribed time period of 40 days. The Data Protection Compliance Officer will be responsible for implementing the process and for dealing with such requests but all employees should be made of aware of protocol.

Created: January 2006

Updated: May 2008

Version 2

Maureen Williams