General Personal Data Regulations Policy

Established May 25, 2018

Owned by - Data Protection Co-Ordinator

Document History

Issue	Date	Amendment Comment
Issue 1	**25/05/2014**	General Issue

Document Authorisation

Description	Name	Sign
Prepared By:	Mr M Jefkins	
Reviewed By:	Ms L.Ylonen	
Authorised By:	Mr A Bowden	

J&E Hall International

Purpose

The General Data Protection Regulation (GDPR) (EU) 2016/679 aims to protect EU citizens from privacy and data breaches in an increasingly data-driven world. The GDPR clarifies the responsibilities of individuals and companies, especially in collecting data and when to gain consent to use personal data.

This policy is based on laws and regulations related to personal data protection in the EU and the UK, and prescribes the basic rules to be complied with by Employees of the Company when processing personal data. These rules are established for the purpose of protecting and utilizing the personal data of the Company's customers, Employees and others.

Scope

This policy applies to personal data in filing systems, in databases on a system, or which is processed automatically.

Definitions

The meanings of terms used in these regulations are the following;

1. "Anonymisation" refers to an irreversible process that renders identification of the data subject impossible.
2. "Biometric data" refers to personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of the individual, which allow or confirm the unique identification of the individual, such as facial images or fingerprint data.
3. "Consent" of the data subject refers to any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him/her.
4. "Data concerning health" refers to personal data which is related to physical or mental health, including the provision of health care services, and which reveals information about his or her health status. It includes body temperature and pulse rate data.
5. "Data protection impact assessment" refers to an assessment of the impact on personal data resulting from data processing operations, and measures envisaged to address the risks For example When using new technologies, the nature, scope, context and purposes of the processing are taken into account to see if it is likely to result in risk to the rights and freedoms of the individual.
6. "Data subject" refers to an individual who is identified or identifiable, directly or indirectly by referring to the person's name or other identifiers related to this individual.
7. "Employees" refers to persons who engage in the work of the Company within the Company organization under the direct or indirect direction and supervision of the Company. In addition to hired employees it also includes directors, auditors, executive officers, corporate officers, employees of affiliated companies who are working on assignment at the Company, dispatched employees working at the Company based on a worker placement contract concluded with the dispatching organization, and similar persons.
8. "EU region" refers to the EEA (European Economic Area) member states, including the EU member states.
9. "Joint control" refers to determining the purpose and means for joint processing by two or more organizations.
10. "Personal data" refers to any information related to the data subject, including but not limited to name, employee ID number or other identification number, location data, online identifiers (IP address, cookies etc.), credit card number, telephone number and email address.

11. “Personal data breach” refers to a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.
12. “Processing” refers to any operation that is performed on personal data, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
13. “Pseudonymisation” refers to the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data is not attributed to an identified or identifiable natural person.
14. “Right not to be subject to a decision based solely on automated processing” refers to the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning the data subject or similarly significantly affects the data subject (including automated credit investigations, decision of insurance rates, and similar matters).
15. “Right of access by the data subject” refers to the right to obtain as to whether or not personal data concerning him or her are being processed, and where that is the case, access to the personal data and the relevant information.
16. “Right of data portability” refers to the right to receive the personal data concerning the data subject, which the data subject has provided, in a structured, commonly used and machine-readable format and have the right to transmit those data to outside organization without hindrance.
17. “Right to erasure (right to be forgotten)” refers to the right to obtain the erasure of personal data concerning the data subject without undue delay.
18. “Right to object” refers to the right of the data subject to object to the processing of personal data that was collected based on legitimate grounds other than consent etc. of the data subject. This processing includes profiling and direct marketing. “Profiling” here refers to any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to the individual, in particular to analyse or predict aspects concerning that individual's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.
19. “Right to rectification” refers to the right to obtain without undue delay the rectification of inaccurate personal data concerning the data subject.
20. “Right to restriction of processing” refers to the right to restrict the processing of personal data that was provided by the data subject.
21. “SCC” (Standard Contractual Clauses) refers to contracts made pursuant to contract templates that are laid down by the European Commission and which are necessary for the lawful transfer of personal data between companies.
22. “Special categories of personal data” refers to personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying the individual, data concerning health or data concerning the individual's sex life or sexual orientation.
23. “Supervisory authority” refers to an independent public authority which is responsible for monitoring the application of laws and regulations on personal data protection in EU region and is established by the EU member states.
24. “Transfer to non-EEA countries” refers to any actions performed for the purpose of enabling a third party in a third country outside the EU region to receive (and/or process) personal data.
25. “Outside organization” refers to a company, association, or other organization other than the Company and its affiliated companies (where affiliated companies are companies owned or controlled directly or indirectly by Daikin Industries, Ltd.).

Management Framework

The following hierarchy shall be established in order to achieve the purpose of this policy

1) Data Protection Responsible

Data Protection Responsible is in charge of and has the authority for implementation and operation of these regulations in the company. The Daikin president shall serve in this position.

2) Global Data Protection Officer (DPO) and the Global Privacy Officer

Data Protection Officer is appointed by Daikin Industries, Ltd in accordance with EU laws and regulations and shall fulfil the following functions;

- Communication and advice to employees with respect to their obligations prescribed in EU laws and regulations related to the protection of personal data;
- Monitoring to ensure compliance with the Privacy Policy established by the Company concerning EU laws and regulations related to the protection of personal data, and to ensure compliance with these regulations;
- Assignment of responsibilities within the Daikin Group and the Company for compliance with EU laws and regulations related to the protection of personal data;
- Improving the awareness of, training of, and related supervision of employees involved in data processing work;
- Provision of advice related to data protection impact assessments, and monitoring of their execution; and
- Cooperation with the EU region supervisory authority, and responding to inquiries to the supervisory authority.

The Data Protection Responsible, the Data Protection Coordinator, and the Employees shall follow the advice and instructions (including those related to the submission of approval forms and other information) made by the Global Data Protection Officer.

The Global Data Protection Officer appoints the head and the members of the Global Privacy Office, which is to be established directly under, and for the purpose to support, the Global Data Protection Officer.

3) Data Protection Coordinators

Data Protection Coordinators are appointed by the Data Protection Responsible. They assist the Data Protection Responsible in personal data processing within the Company and shall fulfil the following functions;

- Identification of personal data processed in the Company;
- Investigations where personal data is collected, used, and provided;
- Implementation of safeguards for personal data;
- Responding to requests for disclosure and other contact from the data subjects;
- Conducting training within the Company;
- Responding to requests for consultation from the Company Employees etc. in relation to other personal data processing;
- Creating records of processing activities of personal data;

- Making the decision to carry out a data protection impact assessment, and carrying out a data protection assessment based on instructions from the Global Data Protection Officer;
- Completing procedures such as conclusion of an SCC with the transfer destination when personal data is transferred outside the EU region; and
- Keeping records of application forms with respect to personal data and responding to request of submissions thereof from the Global Privacy Office.

Privacy Policy

The Data Protection Responsible shall decide the Privacy Policy, which includes the following items;

1. Matters related to appropriate processing of personal data with consideration for the nature of the personal data processed by the Company and for the contents and scale of the Company's business;
2. Compliance with laws and regulations related to the protection of personal data;
3. Matters related to appropriate safeguards of personal data;
4. Detailed contact information of the Company's Global Data Protection Officer;
5. Purposes of personal data processing and legal basis for such processing;
6. Recipients or the categories of recipients of personal data;
7. Safeguards for transfers of personal data to non-EEA countries if such transfers will occur;
8. Period for which personal data will be stored, or if no period can be decided, then the criteria used to determine that period;
9. Rights of the data subjects; and
10. Notification of cookies etc. used on the Company homepage.

The Data Protection Responsible shall fully communicate the Privacy Policy to all Employees and shall also disclose it on the Company homepage or by similar means.

Privacy by Design and Data Protection Impact Assessments

At the time when products, systems, homepage, and other matters are designed, a study shall be conducted to implement appropriate safeguards in order to comply with the personal data processing principles.

Products, systems, homepages, and other matters shall in general be configured by default so that personal data is not collected for purposes not intended by the data subjects.

Decision to carry out a Data Protection Impact Assessment

When engaging in new personal data processing, the Data Protection Coordinator shall decide whether to carry out a data protection impact assessment in accordance with the methods prescribed in the Procedures, and shall immediately report the result of the decision to the Data Protection Responsible and to the Global Data Protection Officer. When it is difficult for the Data Protection Coordinator to make the decision on his/her own, he/she shall discuss with the Global Data Protection Officer.

Carrying out a Data Protection Impact Assessment

When it is necessary to carry out a data protection impact assessment, the Data Protection Coordinator shall carry out the assessment based on instructions from the Global Data Protection Officer, and shall promptly report its result to the Data Protection Responsible and to the Global Data Protection Officer. The Global Data Protection Officer shall decide whether or not consultation with the supervisory authority is necessary, and shall consult the supervisory authority if necessary.

If there is an important change in the risk conditions from previous data protection impact assessments, the Data Protection Coordinator shall consult with the Global Data Protection Officer. As necessary, the Global Data Protection Officer shall give instructions for carrying out a new data protection impact assessment, and thereon the Data Protection Coordinator shall carry out such new data protection impact assessment based on instructions from the Global Data Protection Officer and shall promptly report its result to the Data Protection Responsible and to the Global Data Protection Officer.

Principles Relating to Processing of Personal Data

Lawfulness, Fairness and Transparency - When processing personal data, the processing shall be carried out lawfully, fairly and in a transparent manner.

Data Minimisation - Personal data that is collected by the Company shall be adequate, relevant, and limited to what is necessary, and shall be limited to data necessary to accomplish the operational purposes.

Purpose Limitation - When collecting personal data, the purpose of data use shall be as specific as possible, and the data shall be processed within the scope of that purpose of use. Reproduction of personal data and provision of it to other divisions in the company shall be limited to the minimum necessary for carrying out operations.

Accuracy - Personal data collected by the Company shall be maintained so that it is accurate within the scope necessary for achieving the purpose of use. Where necessary, it shall be kept up to date. Destruction and erasure shall be carried out by the methods prescribed.

Storage Limitation - Personal data which has exceeded the storage period prescribed in laws and regulations and/or in the rules of the company, personal data which is no longer necessary after the purpose of processing was achieved, and personal data which the data subject requested the erasure of shall be destroyed or erased.

Principles for Collection

When collecting personal data, the purpose of its use shall be notified or disclosed to the data subject, and the written consent of the data subject shall be obtained using clear and plain language prior to the processing and in an intelligible and easy accessible form. However, in the circumstances below, the consent of the data subject is not required. The method of notification or disclosure, the items notified or disclosed and the method for obtaining consent are prescribed in the Procedures;

1. When processing is necessary for the performance of a contract to which the data subject is a party or in order to take steps at the request of the data subject prior to entering into a contract;
2. When processing is necessary for compliance with a legal obligation to which the Company is subject; and
3. When processing is necessary to protect vital interests of the data subject or a third party.

Regardless of the provisions of the preceding paragraph, the exceptions detailed above do not apply when processing special categories of personal data. For this type of personal data, processing is in principle prohibited unless explicit consent from the data subject is obtained for processing for one or more specified purposes.

Processing of special categories of personal data is also permitted where processing is necessary for the purpose of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as authorized by EU law or EU member state law or a collective agreement pursuant to EU member state law providing for appropriate

safeguards for the fundamental rights and the interests of the data subject. Following situations are considered such special categories;

1. When processing is necessary to protect the vital interests of a third party or the data subject where the data subject is physically or legally incapable of giving consent;
2. When processing relates to personal data which are manifestly made public by the data subject;
3. When processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;
4. When obtaining consent, the data subject shall be clearly informed that the data subject has the right to withdraw the consent at any time;
5. The data subject shall not be requested to provide consent to provision of personal data that is unrelated to a service as a requirement for providing the service;
6. When processing personal data of children under the age of 16, the consent of a parent or the person holding parental responsibility shall be obtained; and
7. Records of consent by the data subject shall be stored for the period for which the personal data will be stored

Internal Procedures for Collection of Personal Data

When conducting a new operational measure that involves the direct or indirect collection of personal data from data subjects, an application must be submitted in advance to the Data Protection Coordinator using the form prescribed in the Procedures.

The application in the preceding paragraph shall be examined by the Data Protection Coordinator, and approval for collection shall be given by the Data Protection Responsible.

Data Usage

The use of personal data shall be limited to the scope of the purpose of use, which was notified or disclosed at the time when the data was collected, and the personal data shall not be used for any other purpose.

If the purpose of use should be changed, then notification or disclosure of the changed purpose of use shall be provided to the data subject, and the written consent of the data subject shall be obtained using clear and plain language, and in an intelligible and easy accessible form prior to the further processing. In addition, an application for personal data collection shall be submitted.

Employees who learn of personal data in the course of their work shall not carelessly disclose it to third parties or use it for inappropriate purposes. The same shall apply after the person leaves the position involved with such work.

Safeguards to Prevent Deviation from Purpose of Use

When personal data is provided between divisions in the Company, the Data Protection Coordinator shall communicate the purpose of use and other details of the personal data.

Records of Processing Activities of Personal Data

Each time a new activity involving processing of personal data is started, or such an activity was changed, the Data Protection Coordinator shall record the details, including the following items, in the Registry, and shall maintain the contents of the Registry up to date;

1. Processing activity
2. Processing purpose
3. Categories of personal data
4. In-flows of personal data

The Data Protection Coordinator shall submit the Registry to the Global Privacy Office regularly every 3 months and upon request from the Global Privacy Office.

Anonymisation of Personal Data

When personal data will be used or provided in anonymised form, consult in advance with the Global Privacy Office.

Transfer of Personal Data to Outside Organizations

When a new data processing activity involving the transfer of personal data to an outside organization will be started, check the items listed below in advance. Enter the necessary items in the form prescribed in the Procedures, and submit an advance application to the Data Protection Coordinator;

1. Name of the outside organization
2. Name and other details of the data subject
3. Personal data items
4. Legal basis for the transfer

The application in the preceding paragraph shall be examined by the Data Protection Coordinator, and approval for provision shall be given by the Data Protection Responsible.

When the collection of personal data involves the transfers of personal data to non-EEA countries, the requirements of transferring to non-EEA countries will also be complied with.

Outsourcing of Personal Data Processing

If some or all of personal data processing within the scope of the purpose of use is outsourced, the requirements must be complied with and a contractor that provides sufficient guarantees to implement appropriate technical and organisational measures shall be selected in accordance with the procedure prescribed in the Procedures.

In the case described in the preceding paragraph, a contract related to personal data processing, including restrictions on subcontracting etc., shall be concluded with the contractor by document or equivalent means. This document or equivalent means shall include the terms specified by the Global Privacy Office.

The Data Protection Responsible shall check the conditions of contract compliance by the contractor, and shall carry out the necessary supervision and instruction of the contractor to protect personal data appropriately. The methods for supervision and instruction are prescribed in the Procedures.

Division of Responsibilities for Joint Control

When jointly determining the purposes and means of processing personal data with an outside organization, the requirements above shall be complied with, and the respective duties and responsibilities shall be determined by discussion with the outside organization based on advice received from the Global Data Protection Officer.

Provision of Personal Data to Affiliated Companies

When providing personal data to affiliated companies (i.e. companies directly or indirectly controlled by Daikin Industries, Ltd.), the items described above in Transfer of Personal Data to Outside Organizations, Outsourcing of Personal Data Processing and Division of Responsibilities for Joint Control shall not apply. The Data Protection Coordinator shall confirm that the provision of personal data to such affiliated company is in accordance with the contents of the SCC concluded between the Company and the affiliated company, and shall report to the Global Privacy Office.

Safeguards when Transferring Personal Data to Non-EEA Countries

In general, collected personal data shall not be transferred out of the EU region to non-EEA countries, except in cases of transfers to a country that the European Commission has formally recognised as a country which ensures an adequate level of protection.

If it is necessary for operational reasons to transfer personal data to a non-EEA country, provide one of the appropriate safeguards listed below and create records of the contents;

1. Conclusion of an SCC that was adopted or approved by the European Commission;
2. Compliance with codes of conduct that were drawn up by associations and other bodies representing industry and approved by the supervisory authority;
3. Certifications under a certification mechanism approved by the supervisory authority or the European Data Protection Board.

In any of the circumstances listed below, the safeguards described in the preceding paragraph are not necessary;

1. When the European Commission has decided that the country ensures an adequate level of protection, or when the data subject has explicitly consented to the transfer of personal data to a non-EAA country after being informed of the possible risks resulting from the transfer to a non-EEA country due to the absence of appropriate safeguards;
2. When the transfer to a non-EEA country is necessary for the performance of a contract between the data subject and the Company, or the implementation of pre-contractual measures taken at the data subject's request;
3. When the transfer to a non-EEA country is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the Company and another individual or legal person;
4. When the transfer to a non-EEA country is necessary for the establishment, exercise or defence of legal claims; and
5. When the transfer to a non-EEA country is necessary in order to protect the vital interest of the data subject or other persons where the data subject is physically or legally incapable of giving consent.

Implementation of Technical Measures

The Data Protection Responsible shall implement appropriate technical measures such as those listed below taking into account the risks of varying likelihood and severity for the rights and freedoms of individuals (leakage, loss, unauthorized modification etc.) in accordance with EU personal data security guidelines;

1. Pseudonymisation and encryption of personal data;
2. Security of the current systems and services for processing personal data (confidentiality, integrity, availability);

3. System and service recovery capability and procedures in case trouble occurs; and
4. Procedures for regularly conducting inspections, investigations, and assessments of the results of technical and organizational measures for ensuring the security of the processing.

Implementation of Organizational Measures

The Data Protection Responsible and Data Protection Coordinator shall establish an organizational framework and implement organizational measures including training of Employees etc. in order to comply with EU laws and regulations related to protection of personal data and these regulations.

Destruction of Personal Data

The destruction of documents and other media containing personal data shall be carried out as described below;

- Destroy either by using data erasure software to permanently erase the personal data recorded on the electronic media, or by destroying the electronic media.
- Destroy personal data recorded on paper media by shredding it, by contracting its destruction to a contractor, or incinerating it.

Response to Requests from Data Subjects

For responding to requests, the Data Protection Responsible shall establish the following items and make them available to the data subjects by disclosure on the homepage or other means;

1. Contact point
2. Designated request form
3. Method for confirming the identity of the individual
4. Materials to be presented by the data subject in order to identify the personal data which is the subject of the request

Management of the contact point is performed by the Global Privacy Office. The contact point receives the requests that are listed below from the data subjects. (Hereafter such requests are collectively referred to as "Request(s)".);

1. Requests based on the right of access to the personal data;
2. Requests based on the right to rectification;
3. Requests based on the right to erasure (right to be forgotten);
4. Requests based on the right to restriction of processing;
5. Requests based on the right to data portability;
6. Requests based on the right to object; and
7. Requests based on the right not to be subject to a decision based solely on automated processing.

In any of the circumstances listed below, it is not necessary to comply with the right to erasure (right to be forgotten);

1. When the processing is necessary for exercising the right of freedom of expression and information;
2. When the processing is necessary for compliance with legal obligations that require processing based on EU laws or EU member state laws; and
3. When the processing is necessary for the establishment, exercise, or defence of legal claims.

In any of the circumstances listed below, it is not necessary to comply with the right not to be subject to a decision based solely on automated processing;

1. When the processing is necessary for entering into, or performance of, a contract between the data subject and the Company;
2. When the processing is authorized by EU laws or EU member state law that lays down suitable measures to safeguard the data subject's rights, freedoms, and legitimate interests; and
3. When the processing is based on data subject's explicit consent.

When the Global Privacy Office receives a Request from the data subject concerning his/her personal data, they will first check the identity of the data subject and the personal data, and will then identify the Company which processes that personal data and request an action by the Data Protection Coordinator of that company.

When an entity other than the Global Privacy Office receives a Request, the Data Protection Coordinator of the Company which received the request shall immediately notify the Global Privacy Office and take action in response to the Request.

The Data Protection Coordinator in such company shall take action in response free of charge within one month after receiving the request, following the procedures that are prescribed by the Procedures. If there are any uncertain points in this action, the Data Protection Coordinator shall discuss them with the Global Privacy Office.

If the Data Protection Coordinator decides not to take action in response to a Request from the data subject, he/she shall discuss with the Global Privacy Office and notify the data subject of that fact within one month after the request was received. This notification shall include the reason for not taking action in response to the Request, and the possibility of lodging a complaint with a supervisory authority and seeking judicial remedy.

During the course of responding to a Request, the Data Protection Coordinator shall report at each stage to the Global Privacy Office.

Incident Response

When the Data Protection Coordinator receives a report of a personal data breach from security staff or the person who discovered the breach, he/she shall immediately report the related information, including the contents listed below, to the Data Protection Responsible, Global Privacy Office and the Global Data Protection Officer;

1. Nature of the personal data breach;
2. Categories and approximate numbers of the data subjects concerned;
3. Categories and approximate numbers of the personal data records concerned;
4. Measures taken or proposed to be taken by the Company to address the personal data breach;
5. Measures to mitigate the possible adverse effects resulting from the personal data breach; and
6. Possible consequences resulting from the personal data breach.

The Data Protection Coordinator shall require immediate reporting from the processor when a personal data breach occurs at a processor.

When the Global Privacy Office receives a report, as necessary it shall immediately report the breach to all related group companies. As necessary, the Global Privacy Office shall give instructions to the group

companies related to the data breach and the related group companies shall cooperate in accordance with those instructions.

The Global Data Protection Officer shall decide the necessity of notifying to the supervisory authority, and if necessary shall report notify the supervisory authority not later than 72 hours after having become aware of the personal data breach.

The Global Data Protection Officer shall decide the necessity of communicating to the data subjects, and if necessary shall communicate the data subjects promptly.

The Data Protection Coordinator shall document any personal data breaches, their effects and the remedial action taken, and shall keep that documentation.

Conducting Audits

Audits related to personal data processing shall be carried out based on the Internal Audit Regulations and other materials.