EVAC+CHAIR® INTERNATIONAL
Manufacturing life safety products

Pioneering innovation, creating a safer more inclusive world

Introduction
The General Data Protection Regulation 2016 replaces the EU Data Protection Directive of 1995 and supersedes the laws of individual Member States that were developed in compliance with the Data Protection Directive 95/46/EC. Its purpose is to protect the "rights and freedoms" of natural persons (i.e. living individuals) and to ensure that personal data is not processed without their knowledge, and, wherever possible, that it is processed with their consent.

Why this policy exists
To set a standard by which Evac+Chair International will comply with GDPR legislation and lay down how Evac+Chair International interprets GDPR in the context of the work we do.

Policy scope
All processing of personal data by Evac+Chair International is within the scope of this procedure.

Introduction

1.1 Definitions used by the organisation (drawn from the GDPR)

Material scope (Article 2) – the GDPR applies to the processing of personal data wholly or partly by automated means (i.e. by computer) and to the processing other than by automated means of personal data (i.e. paper records) that form part of a filing system or are intended to form part of a filing system.

Territorial scope (Article 3) – the GDPR will apply to all controllers that are established in the EU (European Union) who process the personal data of data subjects, in the context of that establishment. It will also apply to controllers outside of the EU that process personal data in order to offer goods and services, or monitor the behaviour of data subjects who are resident in the EU.

Article 4 Definitions

Establishment – the main establishment of the controller in the EU will be the place in which the controller makes the main decisions as to the purpose and means of its data processing activities. The main establishment of a processor in the EU will be its administrative centre. If a controller is based outside the EU, it will have to appoint a representative in the jurisdiction in which the controller operates to act on behalf of the controller and deal with supervisory authorities.

Personal data – any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. Special categories of personal data – 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 a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

Data controller – the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.

Data subject – any living individual who is the subject of personal data held by an organisation. Processing – any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, 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.

Profiling – is any form of automated processing of personal data intended to evaluate certain personal aspects relating to a natural person, or to analyse or predict that person's performance at work, economic situation, location, health, personal preferences, reliability, or behaviour. This definition is linked to the right of the data subject to object to profiling and a right to be informed about the existence of profiling, of measures based on profiling and the envisaged effects of profiling on the individual.

Personal data breach – 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. There is an obligation on the controller to report personal data breaches to the supervisory authority and where the breach is likely to adversely affect the personal data or privacy of the data subject.

Data subject consent - means 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.

Child – the GDPR defines a child as anyone under the age of 16 years old under UK law. The processing of personal data of a child is only lawful if parental or custodian consent has been obtained. The controller shall make reasonable efforts to verify in such cases that consent is given or authorised by the holder of parental responsibility over the child.

Third party – a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data.

Filing system – any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis.

1.2 The Directors and management of Evac+Chair International, located at Unit 4, Central Boulevard, Blythe Valley Park, Solihull, West Midlands B90 8AW are committed to compliance with all relevant EU and Member State laws in respect of personal data, and the protection of the "rights and freedoms" of individuals whose information Evac+Chair International collects and processes in accordance with the General Data Protection Regulation (GDPR).

1.3 Compliance with the GDPR is described by this policy and other relevant policies such as the Information Security Policy, along with connected processes and procedures.

1.4 The GDPR and this policy apply to all of Evac+Chair International's personal data processing functions, including those performed on customers', clients', employees', suppliers' and partners' personal data, and any other personal data the organisation processes from any source.

1.5 The Information Governance Team is responsible for reviewing the register of processing annually in the light of any changes to Evac+Chair International's activities (as determined by changes to the data inventory register and the management review) and to any additional requirements identified by means of data protection impact assessments. This register will be available on the supervisory authority's request.

1.6 This policy applies to all Employees of Evac+Chair International and any individuals or organisations processing data on behalf of Evac+Chair International. Any breach of the GDPR or this policy will be dealt with under Evac+Chair International's disciplinary policy and may also be a criminal offence, in which case the matter will be reported as soon as possible to the appropriate authorities.

1.7 Partners and any third parties working with or for Evac+Chair International, and who have or may have access to personal data, will be expected to have read, understood and to comply with this policy. No third party may access personal data held by Evac+Chair International without having first entered into a data confidentiality agreement, which imposes on the third-party obligations no less onerous than those to which Evac+Chair International is committed, and which gives Evac+Chair International the right to audit compliance with the agreement.

Policy statement

Responsibilities and roles under GDPR

2.1 Evac+Chair International is a data controller under the GDPR. 2.2 Top Management and all those in managerial or supervisory roles throughout Evac+Chair International are responsible for developing and encouraging good information handling practices within Evac+Chair International.

2.3 The Information Governance Team is accountable to the Directors of Evac+Chair International for the management of personal data within Evac+Chair International and for ensuring that compliance with data protection legislation and good practice can be demonstrated. This accountability includes: 2.3.1 development and implementation of the GDPR as required by this policy; and

2.3.2 Security and risk management in relation to compliance with the policy.

2.4 The Information Governance Team, who Directors considers to be suitably qualified and experienced, has been appointed to take responsibility for Evac+Chair International's compliance with this policy on a day-today basis and, in particular, has direct responsibility for ensuring that Evac+Chair International complies with the GDPR, as do Manager's in respect of data processing that takes place within their area of responsibility.

2.5 The Information Governance Team have specific responsibilities in respect of procedures such as the Subject Access Request Procedure and are the first point of call for Employees seeking clarification on any aspect of data protection compliance.

2.6 Compliance with data protection legislation is the responsibility of all Employees of Evac+Chair International who process personal data.

2.7 Evac+Chair International's Training Policy sets out specific training and awareness requirements in relation to specific roles and Employees of Evac+Chair International generally.

2.8 Employees of Evac+Chair International are responsible for ensuring that any personal data about them and supplied by them to Evac+Chair International is accurate and up-to-date.

2.9 More information on roles and responsibilities for information governance can be located in the Evac+Chair International ISMS (Information Security Management System).

Data protection principles

All processing of personal data must be conducted in accordance with the data protection principles as set out in Article 5 of the GDPR. Evac+Chair International's policies and procedures are designed to ensure compliance with the principles.

3.1 Personal data must be processed lawfully, fairly and transparently 3.1.1 the identity and the contact details of the controller and, if any, of the controller's representative;

3.1.2 The contact details of the Information Governance Team;

3.1.3 The purposes of the processing for which the personal data are intended as well as the legal basis for the processing;

3.1.4 The period for which the personal data will be stored;

3.1.5 The existence of the rights to request access, rectification, erasure or to object to the processing, and the conditions (or lack of) relating to exercising these rights, such as whether the lawfulness of previous processing will be affected;

3.1.6 The categories of personal data concerned;

3.1.7 The recipients or categories of recipients of the personal data, where applicable;

3.1.8 Where applicable, that the controller intends to transfer personal data to a recipient in a third country and the level of protection afforded to the data;

3.1.9 Any further information necessary to guarantee fair processing.

Lawful – identify a lawful basis before you can process personal data. These are often referred to as the "conditions for processing", for example consent.

Fairly – in order for processing to be fair, the data controller has to make certain information available to the data subjects as practicable. This applies whether the personal data was obtained directly from the data subjects or from other sources.

Transparently – the GDPR includes rules on giving privacy information to data subjects in Articles 12, 13 and 14. These are detailed and specific, placing an emphasis on making privacy notices understandable and accessible.

Information must be communicated to the data subject in an intelligible form using clear and plain language. Evac+Chair International's Privacy Notice Procedure is set out in (Appendix A –) and the Privacy Notice is recorded in the Evac+Chair International ISMS.

The specific information that will be provided to the data subject will, as a minimum, include:

3.2 Personal data can only be collected for specific, explicit and legitimate purposes.

3.3 Personal data must be adequate, relevant and limited to what is necessary for processing.

3.3.1 The Information Governance Team is responsible for ensuring that Evac+Chair International does not collect information that is not strictly necessary for the purpose for which it is obtained.

3.3.2 All data collection forms (electronic or paper-based), including data collection requirements in new information systems, will include a fair processing statement or link to privacy statement and approved by the Information Governance Team.

3.3.3 The Information Governance Team will ensure that, on an annual basis all data collection methods are reviewed by internal audit to ensure that collected data continues to be adequate, relevant and not excessive.

3.4 Personal data must be accurate and kept up to date with every effort to erase or rectify without delay.

3.4.1 Data that is stored by the data controller will be reviewed and updated as necessary. No data should be kept unless it is reasonable to assume that it is accurate.

3.4.2 The Information Governance Team is responsible for ensuring that all staff are trained in the importance of collecting accurate data and maintaining it.

3.4.3 It is also the responsibility of the data subject to ensure that data held by Evac+Chair International is accurate and up to date.

3.4.4 Employees, clients and consultants working with Evac+Chair International should be required to notify Evac+Chair International of any changes in circumstance to enable personal records to be updated accordingly. It is the responsibility of Evac+Chair International to ensure that any notification regarding change of circumstances is recorded and acted upon.

3.4.5 The Information Governance Team is responsible for ensuring that appropriate procedures and policies are in place to keep personal data accurate and up to date, taking into account the volume of data collected, the speed with which it might change and any other relevant factors.

3.4.6 On at least an annual basis, the Information Governance Team will review the retention dates of all the personal data processed by Evac+Chair International, by reference to the data inventory, and will identify any data that is no longer required in the context of the registered purpose.

3.4.7 The Information Governance Team is responsible for responding to requests for rectification from data subjects within one month according to the Subject Access Request Procedure. This can be extended to a further two months for complex requests. If Evac+Chair International decides not to comply with the request, a Director will respond to the data subject to explain its reasoning and inform them of their right to complain to the supervisory authority and seek judicial remedy.

3.4.8 A Director is responsible for making appropriate arrangements that, where third-party organisations may have been passed inaccurate or out-of-date personal data, to inform them that the information is inaccurate and/or out of date and is not to be used to inform decisions about the individuals concerned; and for passing any correction to the personal data to the third party where this is required.

Data obtained for specified purposes will not be used for a purpose that differs from those formally documented and communicated as part of Evac+Chair International's GDPR register of processing.

3.5 Personal data must be kept in a form such that the data subject can be identified only as long as is necessary for processing. 3.5.1 Where personal data is retained beyond the processing date, it will be aggregated or anonymized in order to protect the identity of the data subject in the event of a data breach.

3.5.2 Personal data will be retained in line with the limits defined in the data register, once its retention date is passed, it will be securely destroyed.

3.5.3 The Information Governance Team must specifically approve any data retention that exceeds the retention periods defined and must ensure that the justification is clearly identified and in line with the requirements of the data protection legislation.

3.6 Personal data must be processed in a manner that ensures the appropriate security.

3.7 The controller must be able to demonstrate compliance with the GDPR's other principles (accountability).

The Information Governance Team carry out risk assessments taking into account all the circumstances of Evac +Chair International's controlling or processing operations.

In determining appropriateness, the Information Governance Team also consider the extent of possible damage or loss that might be caused to individuals (e.g. staff or customers) if a security breach occurs, the effect of any security breach on Evac+Chair International itself, and any likely reputational damage including the possible loss of customer trust.

The GDPR includes provisions that promote accountability and governance. These complement the GDPR's transparency requirements. The accountability principle in Article 5(2) requires you to demonstrate that you comply with the principles and states explicitly that this is your responsibility.

Evac+Chair International demonstrate compliance with the data protection principles by implementing data protection policies, adhering to codes of conduct, implementing technical and organisational measures, as well as adopting techniques such as data protection by design, DPIAs, breach notification procedures and incident response plans.

Data subjects' rights

4.1 Data subjects have the following rights regarding data processing, and the data that is recorded about them:

4.1.1 To make subject access requests regarding the nature of information held and to whom it has been disclosed.

4.1.2 To prevent processing likely to cause damage or distress.

4.1.3 To prevent processing for purposes of direct marketing.

4.1.4 To be informed about the mechanics of automated decision-taking process that will significantly affect them.

4.1.5 To not have significant decisions that will affect them taken solely by automated process.

4.1.6 To sue for compensation if they suffer damage by any contravention of the GDPR.

4.1.7 To take action to rectify, block, erased, including the right to be forgotten, or destroy inaccurate data.

4.1.8 To request the supervisory authority to assess whether any provision of the GDPR has been contravened.

4.1.9 To have personal data provided to them in a structured, commonly used and machine-readable format, and the right to have that data transmitted to another controller.

4.1.10 To object to any automated profiling that is occurring without consent.

4.2 Evac+Chair International ensures that data subjects may exercise these rights:

4.2.1 Data subjects may make data access requests as described in Subject Access Request Procedure; this procedure also describes how Evac+Chair International will ensure that its response to the data access request complies with the requirements of the GDPR.

4.2.2 Data subjects have the right to complain to Evac+Chair International related to the processing of their personal data, the handling of a request from a data subject and appeals from a data subject on how complaints have been handled in line with the Complaints Procedure.

Consent

5.1 Evac+Chair International understands 'consent' to mean that it has been explicitly and freely given, and a specific, informed and unambiguous indication of the data subject's wishes that, by statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her. The data subject can withdraw their consent at any time.

5.2 Evac+Chair International understands 'consent' to mean that the data subject has been fully informed of the intended processing and has signified their agreement, while in a fit state of mind to do so and without pressure being exerted upon them. Consent obtained under duress or on the basis of misleading information will not be a valid basis for processing.

5.3 There must be some active communication between the parties to demonstrate active consent. Consent cannot be inferred from non-response to a communication. The Controller must be able to demonstrate that consent was obtained for the processing operation.

5.4 For sensitive data, explicit written consent of data subjects will be obtained unless an alternative legitimate basis for processing exists.

5.5 In most instances, consent to process personal and sensitive data is obtained routinely by Evac+Chair International using standard consent documents e.g. when a new client signs a contract, or during induction for participants on programmes.

5.6 Where Evac+Chair International provides online services to children, parental or custodial authorisation will be obtained. This requirement applies to children under the age of 16.

Security of data

6.1 All Employees are responsible for ensuring that any personal data that Evac+Chair International holds and for which they are responsible, is kept securely and is not under any conditions disclosed to any third party unless that third party has been specifically authorised by Evac+Chair International to receive that information and has entered into a confidentiality agreement.

6.2 All personal data should be accessible only to those who need to use it, and access may only be granted in line with the information security policy and information classification policy.

6.3 All Employees are required to enter into an Acceptable Use Agreement before they are given access to organisational information of any sort, which details rules on screen time-outs.

6.4 Manual records may not be left where they can be accessed by unauthorised personnel and may not be removed from business premises without explicit authorisation. As soon as manual records are no longer required, they will be destroyed or archived as per the documented procedures for that category of data.

6.5 Processing of personal data 'off-site' presents a potentially greater risk of loss, theft or damage to personal data. Staff must be specifically authorised to process data off-site.

Disclosure of data

7.1 Evac+Chair International will ensure that personal data is not disclosed to unauthorised third parties which includes family members, friends, government bodies, and in certain circumstances, the Police. All Employees should exercise caution when asked to disclose personal data held on another individual to a third party. 7.2 All requests to provide data for one of these reasons will be supported by appropriate paperwork and all such disclosures must be specifically authorised by the Information Governance Team.

Retention and disposal of data

8.1 Evac+Chair International shall not keep personal data in a form that permits identification of data subjects for longer a period than is necessary, in relation to the purpose(s) for which the data was originally collected.

8.2 Evac+Chair International may store data for longer periods if the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to the implementation of appropriate technical and organisational measures to safeguard the rights and freedoms of the data subject.

8.3 The retention period for each category of personal data is set out in the data register along with the criteria used to determine this period including any statutory obligations Evac+Chair International has to retain the data.

8.4 Personal data will be disposed of securely in accordance with the sixth principle of the GDPR – processed in an appropriate manner to maintain security, thereby protecting the "rights and freedoms" of data subjects.

Data transfers

9.1 All exports of data from within the European Economic Area (EEA) to non-European Economic Area countries (referred to in the GDPR as 'third countries') are unlawful unless there is an appropriate "level of protection for the fundamental rights of the data subjects".

9.1.1 An adequacy decision.

9.1.2 Privacy Shield

The transfer of personal data outside of the EEA is prohibited unless one or more of the specified safeguards, or exceptions, apply:

The European Commission can and does assess third countries, a territory and/or specific sectors within third countries to assess whether there is an appropriate level of protection for the rights and freedoms of natural persons. In these instances, no authorisation is required.

Countries that are members of the European Economic Area (EEA) but not of the EU are accepted as having met the conditions for an adequacy decision.

If Evac+Chair International wishes to transfer personal data from the EU to an organisation in the United States it should check that the organisation is signed up with the Privacy Shield framework at the U.S. Department of Commerce.

9.1.3 Exceptions

Obligation applying to companies under the Privacy Shield are contained in the "Privacy Principles". The US DOC is responsible for managing and administering the Privacy Shield and ensuring that companies live up to their commitments. In order to be able to certify, companies must have a privacy policy in line with the Privacy Principles e.g. use, store and further transfer the personal data according to a strong set of data protection rules and safeguards.

The protection given to the personal data applies regardless of whether the personal data is related to an EU resident or not. Organisations must renew their "membership" to the Privacy Shield on an annual basis. If they do not, they can no longer receive and use personal data from the EU under that framework.

In the absence of an adequacy decision, Privacy Shield membership, binding corporate rules and/or model contract clauses, a transfer of personal data to a third country or international organisation shall only take place on one of the following conditions:

- the data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards;
- the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request;
- the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person;
- the transfer is necessary for important reasons of public interest;
- the transfer is necessary for the establishment, exercise or defence of legal claims; and/or
- the transfer is necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent.

Information asset register/data inventory

10.1 Evac+Chair International has established a data inventory and data flow process as part of its approach to address risks and opportunities throughout its GDPR compliance project. Evac+Chair International's data inventory and data flow determines:

- business processes that use personal data;
- source of personal data;
- volume of data subjects;
- categories of personal data;
- documents the purpose(s) for which each category of personal data is used;
- recipients, and potential recipients, of the personal data; ▪ key systems and repositories;
- any data transfers; and all retention and disposal requirements.

10.2 Evac+Chair International is aware of any risks associated with the processing of particular types of personal data.

10.2.1 Evac+Chair International assesses the level of risk to individuals associated with the processing of their personal data. Data protection impact assessments are carried out in relation to the processing of personal data by Evac+Chair International, and in relation to processing undertaken by other organisations on behalf of Evac+Chair International.

10.2.2 Evac+Chair International shall manage any risks identified by the risk assessment in order to reduce the likelihood of a non-conformance with this policy.

10.2.3 Where a type of processing, in particular using new technologies and taking into account the nature, scope, context and purposes of the processing is likely to result in a high risk to the rights and freedoms of natural persons, Evac+Chair International shall, prior to the processing, carry out a DPIA of the impact of the envisaged processing operations on the protection of personal data. A single DPIA may address a set of similar processing operations that present similar high risks.

10.2.4 Where, as a result of a DPIA it is clear that Evac+Chair International is about to commence processing of personal data that could cause damage and/or distress to the data subjects, the decision as to whether or not Evac+Chair International may proceed will be escalated for review to the Information Governance Team.

10.2.5 The Information Governance Team shall, if there are significant concerns, either as to the potential damage or distress, or the quantity of data concerned, escalate the matter to the supervisory authority.

10.2.6 Appropriate controls will be selected and applied to reduce the level of risk associated with processing individual data to an acceptable level, by reference to the requirements of the GDPR.

Appendix A – Article 12

a. Evac+Chair International identifies the legal basis for processing personal data before any processing operations take place by clearly establishing, defining and documenting: i. the specific purpose of processing the personal data and the legal basis to process the data under:

1. Consent obtained from the data subject; 1. explicit consent obtained from the data subject;
2. Necessary for employment rights or obligations;
3. Protect the vital interests of the data subject, including the protection of rights and freedoms;
4. Necessary for the legitimate activities with appropriate safeguards;
5. Personal data made public by the data subject;
6. Legal claims;
7. Substantial public interest;
8. Preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, provision of health or social care treatment, or management of health and social care systems and services, under the basis that appropriate contracts with health professionals and safeguards are in place;
9. Public health, ensuring appropriate safeguards are in place for the protection of rights and Freedoms of the data subject, or professional secrecy;
10. National laws in terms of processing genetic, biometric health data.

2. Performance of a contract where the data subject is a party;
3. Legal obligation that Evac+Chair International is required to meet;
4. Protect the vital interests of the data subject, including the protection of rights and freedoms;
5. Official authority of Evac+Chair International or to carry out the processing that is in the public interest;
6. Necessary for the legitimate interests of the data controller or third party, unless the processing is overridden by the vital interests, including rights and freedoms;
7. National law.

ii. Any special categories of personal data processed and the legal basis to process the data under:

Appendix A- Privacy notices

b. When personal data collected from data subject with consent i. Evac+Chair International is transparent in its processing of personal data and provides the data subject with the following:

1. Evac+Chair International's identity, and contact details and any data protection representatives;
2. The purpose(s), including legal basis, for the intended processing of personal data

3. Where relevant, Evac+Chair International's legitimate interests that provide the legal basis for the processing;
4. Potential recipients of personal data;
5. Any information regarding the intention to disclose personal data to third parties and whether it is transferred outside the EU. In such circumstances, Evac+Chair International will provide information on the safeguards in place and how the data subject can also obtain a copy of these safeguards;
6. If Evac+Chair International is based outside of the EU and the data subject resides within it (the EU), the Evac+Chair International provides the data subject with contact details of a data protection representative in the EU;
7. Any information on website technologies used to collect personal data about the data subject;
8. Any other information required to demonstrate that the processing is fair and transparent.
ii. All information provided to the data subject is in an easily accessible format using clear and plain language.
iii. Privacy notices for personal data processing is recorded

b. When data is contractually required for processing

i. Evac+Chair International processes data without consent in order to fulfil contractual obligations. For example, employee details, supplier details.
ii. Privacy notice for this personal data processing is recorded (GDPR REC 4.1)

c. When personal data has been obtained from a source other than the data subject i. Evac+Chair International makes clear the types of information collected as well as the source of the personal data (publicly accessible sources) and provides the data subject with:

1. Evac+Chair International's (data controller) identity, and contact details of the data owner and any data protection representatives;
2. The purpose(s), including legal basis, for the intended processing of personal data;
3. Categories of personal data;
4. Potential recipients of personal data;
5. Any information regarding disclosing personal data to third parties and whether it is transferred outside the EU – Evac+Chair International will provide information on the safeguards in place and how the data subject can also obtain a copy of these safeguards;
6. Any other information required to demonstrate that the processing is fair and transparent.

Privacy notice for this personal data processing is recorded (GDPR REC 4.1).