# MWC GROUP UK

# DATA PROTECTION/PRIVACY POLICY

# CONTENTS

# 1. INTRODUCTION

This Policy outlines our legal requirements under data protection laws, in particular the General Data Protection Regulation (GDPR) (Regulation EU 2016/679) and the Data Protection Act 2018 and the processes which MWC Group UK (the "Company" or "MWC") is to follow in order to meet them. The General Data Protection Regulation (GDPR) is the primary data protection regulation for the United Kingdom.

The GDPR is a European Union regulation that governs the protection of personal data, and it applies to EU member states, including the UK. After the UK's departure from the EU, it retained the GDPR as part of its domestic law with some modifications. In the UK, the GDPR is complemented by the Data Protection Act 2018.

During its daily operations, the Company controls and processes personal data pertaining to its clients, employees, and other individuals for a variety of business purposes. In this regard, the Company is considered to be a "Controller" and a "Processor" under the GDPR. As Controller and/or Processor, the Company is required to process such data in accordance with the GDPR.

The purpose of this Policy is to set out the Company's commitment and procedures for protecting personal data. The Company regards the correct and lawful treatment of personal data as a priority and as essential in maintaining confidence of its employees, clients and related third parties.

This Policy refers to the processing of personal data in relation to natural persons and does not apply to data pertaining to legal persons such as Company.

For clarifications on the content of these Policies and Procedures, please contact the Data Protection Officer/Representative of the Company.

These Policies and Procedures shall be reviewed once a year and any changes approved by the Board of Directors.

This Data Protection Policy is owned and approved by the Board of Directors of MWC. The responsibility for the day-to-day implementation of the Policy lies with the respective Board of Directors of each entity within the Group.

# 2. DEFINITIONS

The definitions below are verbatim as per the 'General Data Protection Regulation'.

1. 'personal data' means any information relating to an identified or identifiable natural person ('data subject'), which in the context of the MWC Group mainly refers to prospective, and current clients, beneficiaries, and employees of the MWC Group,

2. 'processing' means any operation or set of operations which is performed on personal data or on sets of personal data,

3. 'restriction of processing' means the marking of stored personal data with the aim of limiting their processing in the future.

4. 'profiling' means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person,

5. 'pseudonymisation' means 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 'key' information,

6. 'filing system' means any structured set of personal data which are accessible according to specific criteria,

7. 'controller' refers to MWC Group which, determines the purposes and means of the processing of personal data.

8. 'processor' means a natural or legal person, or other body, which processes personal data on behalf of the controller. These include the company's Insurance Brokers and outsource service providers who process or have access to personal data.

9. 'recipient' means a natural or legal person, public authority, agency, or another body, to which the personal data are disclosed, whether a third party or not.

10. 'third party' means a natural or legal person, public authority, agency, or body (other than the data subject, controller, processor) who, under the direct authority of the controller or processor, is / are authorised to process personal data.

11. 'consent' of the data subject 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 relating to him or her.

12. 'personal data breach' means 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.

13. 'genetic data' means personal data relating to the inherited or acquired genetic characteristics of a natural person.

14. ‘biometric data’ means personal data resulting from specific technical processing relating to the physical, physiological, or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data.

15. ‘data concerning health’ means personal data related to the physical or mental health of a natural person,

16. ‘representative’ means a natural or legal person who is designated by the controller or processor in writing and represents the controller or processor with regard to their respective obligations.

17. ‘enterprise’ means a natural or legal person engaged in an economic activity, irrespective of its legal form, including partnerships or associations regularly engaged in an economic activity.

18. ‘group of undertakings’ means a controlling undertaking and its controlled undertakings.

19. ‘binding corporate rules’ means personal data protection policies which are adhered to by a controller or processor established on the territory of a Member State for transfers or a set of transfers of personal data to a controller or processor in one or more third countries within a group of undertakings, or group of enterprises engaged in a joint economic activity.

20. ‘supervisory authority’ means an independent public authority which is established by a Member State pursuant to Article 51;

21. ‘supervisory authority concerned’ means a supervisory authority which is concerned by the processing of personal data because:

    1. the controller or processor is established on the territory of the Member State of that supervisory authority.

    2. data subjects residing in the Member State of that supervisory authority are substantially affected or likely to be substantially affected by the processing; or

    3. a complaint has been lodged with that supervisory authority.

22. ‘cross-border processing’ means either:

    1. processing of personal data which takes place in the context of the activities of establishments in more than one Member State of a controller or processor in the Union where the controller or processor is established in more than one Member State: or

    2. processing of personal data which takes place in the context of the activities of a single establishment of a controller or processor in the Union, but which substantially affects or is likely to substantially affect data subjects in more than one Member State.

23. 'relevant and reasoned objection' means an objection to a draft decision as to whether there is an infringement of this Regulation, or whether envisaged action in relation to the controller or processor complies with this Regulation, which clearly demonstrates the significance of the risks posed by the draft decision as regards the fundamental rights and freedoms of data subjects and, where applicable, the free flow of personal data within the Union.

24. 'information society service' means a service as defined in point (b) of Article 1(1) of Directive (EU) 2015/1535 of the European Parliament and of the Council ([1]);

25. 'international organisation' means an organisation and its subordinate bodies governed by public international law, or any other body which is set up by, or on the basis of, an agreement between two or more countries.

26. 'public authority and public body' for the purposes of the GDPR, the following (and only the following) are "public authorities" and "public bodies" under the law of the United Kingdom.

Note: In this policy, the word '**company**' has been used to mean, MWC Group UK.

# 3. RESPONSIBILITIES

**The Board of Directors**

The Board of Directors are responsible to ensure that this policy is adhered to, updated as required, implemented, and that the company has the resources necessary to implement this policy.

The Board of Directors shall ensure the implementation of appropriate technical and organisational measures in order to be able to demonstrate that processing is performed in accordance with the GDPR. Any such measures shall be reviewed and updated where necessary.

The Board shall also ensure adherence to approved codes of conduct as referred to in Article 40 or approved certification mechanisms as referred to in Article 42 of the GDPR which may be used to demonstrate compliance with the obligations of the Company under the GDPR.

**The Senior Managers ("SM")**

The SM are responsible for ensuring that the infrastructure of the company is adequate to cater for the implementation of this policy and that the operational units comply with the requirements of this policy. The responsibility of the SM are also extended to any outsource service provider that the company might use for any outsourced service in respect of the obligations under the GDPR.

The SM shall ensure that the company has updated data processing charts of all personal data, which shall include:

1. A record of the processing activities under their responsibility containing all of the following information:

    i. the name and contact details of the company and where applicable any joint controllers (and their representatives), and the name of the Data Protection Officer.

    ii. the purposes / reasons of the processing of any personal data.

    iii. a description of the categories of data subjects and of the categories of personal data.

    iv. the categories of recipients to whom the personal data have been or will be disclosed to including recipients in third countries or international organization's if and where applicable.

    v. where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, documentation of suitable safeguards that have been put into place for these transfers.

    vi. the retention period time limits for the different categories of personal data (please refer to the Retention Sub-Policy.

    vii. a general description of the technical and organisational security measures that the Company has put into place.

2. A record of all categories of processing activities carried out on behalf of the company, containing:

    i. the name and contact details of the processor or processors and of each controller on behalf of which the processor is acting, and, where applicable, of the controller's or the processor's representative, and the name of the data protection officer.

    ii. where applicable, transfers of personal data to a third country or an international organization, including the identification of that third country or international organization and the documentation of suitable safeguards.

iii. where possible, a general description of the technical and organizational security measures.

3. The records referred to in paragraphs 1 and 2 above shall be in writing and in electronic form and the company or its processors shall make the records available to the Data Protection Commissioner on request.

The SM must also:

i. Ensure that the physical security on the business premises is adequate to ensure that any personal data cannot leave the office in any form physically or electronically.

ii. Ensure that any personal data is not used for any other purpose than for what it had been originally collected.

iii. Any staff access to personal data should be restricted on a need-to-know basis and there must be adequate measures put into place to ensure that staff cannot access electronic or physical files which contain personal data and which they do not require to fulfil their duties.

iv. Ensure that staff cannot access any personal data in any form through the use of other staff's credentials.

**The Data Protection Officer (DPO)**

The nature of business of the MWC Group and its processors consists of processing operations which, by virtue of their nature, their scope and / or their purposes, require regular and systematic monitoring of data subjects on a large scale and the core activities of the controller or the processor consist of processing on a large scale of special categories of data, and personal data relating to criminal convictions and offences.

For this reason, the group shall appoint a person who will act as a DPO.

i. The DPO must be involved, properly and in a timely manner, in all issues which relate to the protection of personal data throughout the Company.

ii. The Company shall support the DPO in performing his / her tasks by providing any resources that are necessary to carry out those tasks and access to personal data and processing operations and provide access to adequate training to update and maintain his or her expert knowledge.

iii. The Company shall ensure that the DPO has full independence in the exercise of the role and shall not be dismissed or penalised by the company for performing his /her tasks in accordance with the GDPR. The DPO shall directly report to the Board of Directors and shall keep the respective Compliance Manager updated with any matters arising that can have any regulatory implications on any of the Company.

iv. The company must ensure that data subjects have access and are able to contact the DPO directly with regard to all issues related to processing of their personal data

and to the exercise of their rights under the GDPR. For this reason, the name and contact details of the DPO shall be made available by the Company to any data subject asking for this information.

v. The DPO shall be bound by secrecy or confidentiality concerning the performance of his or her tasks,

vi. The DPO may fulfil other tasks and duties, however the company shall ensure that any such tasks and duties do not result in a conflict of interests or impede the DPO from fulfilling his / her role.

**Responsibilities of the DPO**

The DPO will,

i. inform and give advice to the Company, employees, and other processors who carry out processing of their obligations under this Regulation,

ii. monitor the Company compliance with the GDPR, and with any other such data protection rules and regulations, and with the policies of the company in relation to the protection of personal data,

iii. assist the company with the assignment of responsibilities under the GDPR,

iv. be the main lead in regard to awareness-raising and assist with the training of staff involved in processing operations,

v. provide advice were requested as regards any data protection impact assessment and monitor the assessments progression going forward,

vi. cooperate fully with the Data Protection Authority as required,

vii. act as the contact point for the Data Protection Authority on issues relating to processing, including any prior consultation that might be required in accordance with Article 36 of the GDPR where appropriate, and with regard to any other matter,

viii. The DPO shall in the performance of his or her tasks have due regard to the risk associated with processing operations, taking into account the nature, scope, context, and purposes of processing.

**The Group Head Compliance**

The Group Head of Compliance must ensure that the Data Protection Policy and all the procedures contained herein are always adhered to.

**Human Resources Manager (HR Manager) or Compliance Team**

The HR Manager or Compliance Team must ensure that all the employees within the MWC Group are adequately trained and are fully cognisant with the requirements of the General

Data Protection Regulation and the Data Protection Policy of the company and any other guidelines that the company may issue from time to time in this regard.

# 4. PROCESSING OF PERSONAL DATA - GENERAL REQUIREMENTS

MWC Group must ensure that all personal data is:

i. processed lawfully, fairly and in a transparent manner in relation to all data subjects.

ii. collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes for which it has been originally collected.

iii. adequate, relevant, and limited to what is necessary to transact insurance business / investments falling within its subsidiary's regulatory authorization.

iv. accurate, kept up to date, and ensure that every reasonable step must be taken so that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased, or rectified without delay.

v. kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed. Personal data may be stored for longer periods insofar as the personal data will be processed solely historical research purposes or statistical purposes subject to the implementation of the appropriate technical and organisational measures required to safeguard the rights and freedoms of the data subject ('storage limitation').

vi. processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organisational measures.

# 5. LAWFULNESS OF PROCESSING

MWC Group shall only process data if at least one of the following applies:

i. the data subject has given consent to the processing of his or her personal data for one or more specific purposes.

ii. processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract.

iii. processing is necessary for compliance with a legal obligation to which the company is subject.

iv. processing is necessary in order to protect the vital interests of the data subject or of another natural person.

v. processing is necessary for the purposes of the legitimate interests pursued by the company or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

Where the processing for a purpose other than that for which the personal data have been collected is not based on the data subject's consent, the company shall, in order to ascertain whether processing for another purpose is compatible with the purpose for which the personal data are initially collected, take into account the following:

i. any link between the purposes for which the personal data had originally been collected and the purposes of the intended further processing.

ii. the context in which the personal data had been collected, in particular regarding the relationship between data subjects and the company.

iii. the nature of the personal data, in particular whether special categories of personal data are processed, or whether personal data related to criminal convictions and offences are processed.

iv. the possible consequences of the intended further processing for data subjects.

v. the existence of appropriate safeguards, which may include encryption or pseudonymisation.

## 5.1 Obtaining consent for processing, and conditions for consent.

i. The company must always ensure that it is able to demonstrate that the data subject has consented to processing of his or her personal data.

ii. Prior to giving consent, the data subject shall be informed of the meaning of granting consent for the processing of his / her personal data.

iii. If the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language.

iv. The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal.

v. When assessing whether consent is freely given, due consideration shall be taken of whether, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract.

### 5.2 Obtaining a child's consent for data processing.

i. The company shall not process the personal data of a child unless the child is at least 16 years old.

ii. Where the child is below the age of 16 years, such processing shall be lawful only if and to the extent that consent is given or authorised by the holder of parental responsibility over the child.

iii. 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.

## 6. THE PROCESSING OF SPECIAL CATEGORIES OF PERSONAL DATA

1. Processing of 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 is prohibited under the GDPR.

2. Paragraph 1 shall not apply if one of the following applies:

    i. the data subject has given explicit consent to the company for the processing of those personal data for one or more specified purposes,

    ii. processing is necessary for the purposes of carrying out the obligations and exercising specific rights of MWC Group or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by Union or Member State law or a collective agreement pursuant

to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject.

iii. processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent.

iv. processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects;

v. processing relates to personal data which are manifestly made public by the data subject.

vi. processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity.

vii. processing is necessary for the assessment of the working capacity of the employee, subject to the conditions and safeguards referred to in paragraph 3.

viii. processing is necessary for archiving purposes or statistical purposes and respect the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

# 7. PROCESSING OF PERSONAL DATA RELATED TO CRIMINAL CONVICTIONS

In determining whether to provide insurance / investment services, MWC Group may.

(i) request a proposer to disclose any data relating to his criminal convictions or to submit a conduct certificate by the Police together with the proposal form.
(ii) conduct internet searches on a particular person to obtain additional background information which will enable MWC Group to make a decision on whether to provide insurance cover or not.

If the proposer has a criminal record and in the opinion of MWC Group such record constitutes a reasonable ground for refusal of an insurance cover, MWC Group may opt not to issue such cover.

The collection and processing of personal data relating to criminal convictions is to comply with Article 60 of the Insurance Business Act which permits sharing of information for the purpose of preventing, detecting, or suppressing insurance fraud.

Additionally, MWC Group is deemed to be a subject person conducting a relevant activity in terms of the Article (2)(1) of the Prevention of Money Laundering and Funding of Terrorism Regulations S.L 373.01 and is therefore required to collect and process personal data relating to criminal convictions in order to comply with its legal obligations.

MWC Group is required to ensure that it undertakes measures to ensure that such processing is proportional having regard to the reason why it was collected.

# 8. PROCESSING THAT DOES NOT REQUIRE IDENTIFICATION

1. If the purposes for which a company processes personal data do not or do no longer require the identification of a data subject by the company, the company shall not be obliged to maintain, acquire, or process additional information in order to identify the data subject for the sole purpose of complying with the GDPR.

2. Where, in cases referred to in paragraph 1 above, the company can demonstrate that it is not in a position to identify the data subject, the company shall inform the data subject accordingly, if possible unless the data subject provides additional information enabling his or her identification.

# 9. INFORMATION THAT MUST BE GIVEN TO THE DATA SUBJECT DURING THE PROCESS OF DATA COLLECTION

1. Where personal data relating to a data subject is collected from the data subject, the company must ensure that the data subject is provided with all the following information:

i. the identity and the contact details of the company and, the controller's representative.

ii. the contact details of the DPO.

iii. the purposes of the processing for which the personal data are intended as well as the legal basis for the processing.

iv. the legitimate interests pursued by the controller or by a third party in collecting the data.

v. the recipients or categories of recipients of the personal data that has been collected.

vi. where applicable, the fact that the company transfers OR, intends to transfer personal data to a third country or international organisation and the existence or absence of an adequacy decision by the Commission, or in the case of transfers referred to in Article 46 or 47, or the second subparagraph of Article 49(1), reference to the appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available.

vii. the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period.

viii. the existence of the right to request from the company access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability.

ix. where the processing is based on point (a) of Article 6(1) or point (a) of Article 9(2), the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;

x. the right to lodge a complaint with the DPC.

xi. whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data.

xii. the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

2. In cases where the company intends to further process the personal data for a purpose other than that for which the personal data were collected, the company shall provide the data subject prior to that further processing with information on that other purpose and with any relevant further information.

A copy of the company's privacy notice is attached in **APPENDIX 1.**

# 10. INSTANCES WHERE PERSONAL DATA IS NOT OBTAINED FROM THE DATA SUBJECT

1. Where personal data have not been obtained from the data subject, the company shall provide the data subject with the following information in addition to (i) to (xii) above and,

2. details as to from which source the personal data originate, and if applicable, whether it came from publicly accessible sources.

3. The company shall provide the information referred to in paragraphs 1 and 2:

    i. within a reasonable period after obtaining the personal data, but at the latest within one month, having regard to the specific circumstances in which the personal data are processed.

    ii. if the personal data are to be used for communication with the data subject, at the latest at the time of the first communication to that data subject; or

    iii. if a disclosure to another recipient is envisaged, at the latest when the personal data are first disclosed.

4. In cases where the company intends to further process the personal data for a purpose other than that for which the personal data were collected, the company shall provide the data subject prior to that further processing with information on that other purpose and with any relevant further information.

# 11. RIGHTS OF DATA SUBJECTS – SPECIFIC RIGHTS.

## 11.1 Right of access to own personal data by data subjects.

1. Data subject shall have the right to obtain from the company confirmation as to whether personal data concerning him or her are being processed, and where that is the case, access to the personal data and the following information:

    i. the purposes of the processing.

    ii. the categories of personal data concerned.

    iii. the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations.

    iv. where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period.

v. the existence of the right to request from the company rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing.

vi. the right to lodge a complaint with the DPC.

vii. where the personal data are not collected from the data subject, any available information as to their source.

viii. the existence of automated decision-making, including profiling, and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

2. Where personal data are transferred to a third country or to an international organisation, the data subject shall have the right to be informed of the appropriate safeguards that the company has put into place relating to the transfer.

3. The company shall provide a copy of the personal data undergoing processing. The company may charge a reasonable fee based on administrative costs. Where the data subject makes the request by electronic means, and unless otherwise requested by the data subject, the information shall be provided in a commonly used electronic form.

4. The right to obtain a copy referred to in paragraph 3 shall not adversely affect the rights and freedoms of other data subjects.

5. The company shall provide any information on action taken on a request by a data subject without undue delay and in any event within one month of receipt of the request. That period may be extended by two further months where necessary, taking into account the complexity and number of the requests.

6. The company shall inform the data subject of any such extension within one month of receipt of the request, together with the reasons for the delay. Where the data subject makes the request by electronic form means, the information shall be provided by electronic means where possible, unless otherwise requested by the data subject.

7. If the company does not take action on the request of the data subject, the company shall inform the data subject without delay and at the latest within one month of receipt of the request of the reasons for not taking action and on the possibility of lodging a complaint with the Data Protection Commissioner and seek a judicial remedy.

8. Any information provided to data subjects and any communication and any actions taken to comply with the GDPR shall be provided free of charge, however where requests from a data subject are manifestly unfounded or excessive, in particular because of their repetitive character, the company may either:

i. charge a reasonable fee taking into account the administrative costs of providing the information or communication or taking the action requested; or

ii. refuse to act on the request.

The company shall bear the burden of demonstrating the unfounded or excessive character of the data subject's request.

9. In exercising the rights of the data subject, the company may request the provision of additional information necessary to confirm the identity of the data subject before complying with any request.

All such requests for rectification must be immediately channeled to the DPO of the MWC Group.

## 11.2 Right to rectification.

Data subjects shall have the right to ask for the rectification of inaccurate personal data concerning him or her. Taking into account the purposes of the processing, the data subject shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement.

All such requests for rectification must be immediately channeled to the DPO of the MWC Group.

## 11.3 Right to be forgotten.

1. The data subject shall have the right to obtain from the company the erasure of personal data concerning him or her without undue delay and the company shall have the obligation to erase personal data without undue delay where one of the following grounds applies:

    i. the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed.

    ii. the data subject withdraws consent on which the processing is based and where there is no other legal ground for the processing.

    iii. the data subject objects to the processing and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing for marketing purposes.

    iv. the personal data have been unlawfully processed.

    v. the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the company is subject.

2. Where any one of the Company has made the personal data public (or made available to processors) and is obliged to erase the personal data, the company, taking account of available technology and the cost of implementation, shall take

reasonable steps, including technical measures, to inform other controllers and processors which are processing the personal data that the data subject has requested the erasure by such controllers of any links to, or copy or replication of, those personal data.

3. Paragraphs 1 and 2 shall not apply to the extent that processing is necessary:

    i. for compliance with a legal obligation which requires processing by Union or Member State law to which the company is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.
    ii. for statistical purposes.
    iii. for the establishment, exercise, or defense of legal claims.

All such requests for rectification must be immediately channeled to the DPO of the MWC Group.

## 11.4 Right to restriction of processing.

1. The data subject shall have the right to obtain from the company a restriction of processing where one of the following applies:

    i. the accuracy of the personal data is contested by the data subject, for a period enabling the company to verify the accuracy of the personal data.

    ii. the processing is unlawful, and the data subject opposes the erasure of the personal data and requests the restriction of their use instead.

    iii. the company no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise, or defense of legal claims.

    iv. the data subject has objected to processing pending the verification whether the legitimate grounds of the company override those of the data subject.

2. Where processing has been restricted under paragraph 1, such personal data shall, with the exception of storage, only be processed with the data subject's consent or for the establishment, exercise, or defense of legal claims or for the protection of the rights of another natural or legal person.

3. A data subject who has obtained restriction of processing pursuant to paragraph 1 shall be informed by the company before the restriction of processing is lifted.

## 11.5 Right to data portability

1. The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to the company, in a structured, commonly used, and machine-readable format and have the right to transmit those data to another

controller without hindrance from the company to which the personal data have been provided.

2. In exercising his or her right to data portability pursuant to paragraph 1, the data subject shall have the right to have the personal data transmitted directly from one controller to another, where technically feasible.

3. The exercise of the right referred to in paragraph 1 above shall be without prejudice to the right to be forgotten.

4. The right referred to in paragraph 1 shall not adversely affect the rights and freedoms of others.

### 11.6 Right to object

1. The data subject shall have the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her which is based on processing that is necessary for the purposes of the legitimate interests pursued by the company or by a third party. The company shall no longer process the personal data unless the company demonstrates compelling legitimate grounds for the processing which override the interests, rights, and freedoms of the data subject or for the establishment, exercise or defence of legal claims.

2. Where personal data are processed for direct marketing purposes, the data subject shall have the right to object at any time to the processing of personal data concerning him or her for such marketing, which includes profiling to the extent that it is related to such direct marketing.

3. Where the data subject objects to processing for direct marketing purposes, the personal data shall no longer be processed for such purposes.

4. At the latest at the time of the first communication with the data subject, the right referred to in paragraphs 1 and 2 shall be explicitly brought to the attention of the data subject and shall be presented clearly and separately from any other information.

5. The data subject may exercise his or her right to object to the use his / her personal data by automated means.

6. Where personal data are processed for scientific or historical research purposes or statistical purposes, the data subject, on grounds relating to his or her particular situation, shall have the right to object to processing of personal data concerning him or her, unless the processing is necessary for the performance of a task carried out for reasons of public interest.

## 12. PROCESSORS

1. Where any processing is to be carried out on behalf of the company, the company shall use only processors that are able to provide sufficient guarantees to implement

appropriate technical and organisational measures in such a manner that processing will meet the requirements of the GDPR and ensure the protection of the rights of the data subject. Adequate Due Diligence must be carried out on any proposed outsource service providers before any service is obtained from third party processors.

2. The company must ensure that any processor it engages shall not engage another processor without prior specific or general written authorisation of the company. In the case of general written authorisation, the processor shall inform the company of any intended changes concerning the addition or replacement of other processors, thereby giving the company the opportunity to object to such changes before they take effect.

3. Processing by a processor shall be governed by a contract that is binding on the processor with regard to the company and that sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the company. That contract or other legal act shall stipulate, in particular, that the processor:

i. processes the personal data only on documented instructions from the company,

ii. ensures that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

iii. takes all measures required to ensure the security of personal data in the processing.

iv. assists the company by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the controller's obligation to respond to requests for exercising the data subject's rights laid down in the GDPR,

v. assists the company in ensuring compliance with the obligations of the GDPR taking into account the nature of processing and the information available to the processor.

vi. on the instruction of the company, deletes or returns all the personal data to the company after the end of the provision of services relating to processing, and deletes existing copies unless Union or Member State law requires storage of the personal data.

vii. makes available to the company all information necessary to demonstrate compliance with the obligations laid down in this Section and allow for and contribute to audits, including inspections, conducted by the company or another auditor mandated by the company.

4. Where a processor engages another processor for carrying out specific processing activities on behalf of the company, the same data protection obligations as set out in the contract or other legal act between the company and the processor as referred to in paragraph 3 shall be imposed on that other processor by way of a contract or other legal act under Union or Member State law, in particular providing sufficient

guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of this Regulation. Where that other processor fails to fulfil its data protection obligations, the initial processor shall remain fully liable to the company for the performance of that other processor's obligations.

5. Adherence of a processor to an approved code of conduct as referred to in Article 40 of the GDPR or an approved certification mechanism as referred to in Article 42 of the GDPR may be used as an element by which to demonstrate sufficient guarantees as referred to in paragraphs 1 and 4 of this Section.

The processor shall immediately inform the company if, in its opinion, an instruction infringes this Regulation or other Union or Member State data protection provisions.

# 13. AGREEMENTS WITH THIRD PARTIES

The company shall ensure that written agreements are put into place in instances where third parties carry out any processing for the Company and / or its subsidiaries. These include the following instances:

- Insurance Intermediaries and business introducers,
- Insurance Brokers,
- Reinsurers,
- Outsourced service providers,
- External consultants and other service providers who have access to personal data collected by the company,
- And any other such relationship not mentioned above.

# 14. SUB POLICIES

### 1. Breach Policy and Procedure

The company has set up a procedure which is to be followed in the event of a breach of personal data **(see APPENDIX 2)**. A breach would be deemed to happen if any personal data that the company possesses is used for other purpose/s other than for what it had been

originally collected by any other company or processor, employee, any outsource service provider to the Group, or any other third party.

The breach procedure involves two processes:

1. A formal communication to the Data Protection Commissioner, and

2. A formal communication to the data subjects whose data has been used other that for the reason for which it has been collected.

The whole process will be entirely managed by the DPO of the MWC Group.

## Communication to the Data Protection Commissioner:

1. In the case of a personal data breach, the company shall without undue delay and, where feasible, not later than 72 hours after having become aware of the breach, notify the personal data breach to the Data Protection Commissioner (DPC). This notification will not be required if the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. If the notification to the DPC is not made within 72 hours, the company shall give reasons to the DPC for the delay.

2. All processors of the company shall notify the company without undue delay after becoming aware of a personal data breach.

3. The notification referred to in paragraph 1 shall:

    i. describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned, and the categories and approximate number of personal data records concerned.

    ii. communicate the name and contact details of the DPO or other contact point where more information can be obtained.

    iii. describe the likely consequences of the personal data breach.

    iv. describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

4. If it is not possible to provide all of the information to the DPC concurrently, the company may provide the information in phases without undue delay.

5. The company, through the Data Protection Officer, shall document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken. All documentation shall enable the DPC to verify compliance with this Breach policy and procedures.

Communication to data subjects:

1. When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the company through its Data Protection Officer shall communicate the personal data breach to the data subject without undue delay.

2. The communication to the data subject shall describe in clear and plain language the nature of the personal data breach and contain at least the information and measures as follows:

    I. inform the data subjects of the name and contact details of the DPO or other contact point where more information can be obtained.

    II. describe the likely consequences of the personal data breach.

    III. describe the measures taken or proposed to be taken by the company to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

3. The communication to the data subject referred to in paragraph 1 above shall not be required if any of the following conditions are met:

    I. the company has implemented appropriate technical and organisational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that make the personal data unintelligible to any person who is not authorised to access it, such as encryption.

    II. the company has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects referred to in paragraph 1 is no longer likely to materialise.

    III. it would involve disproportionate effort to communicate to all data subjects. In such a case, the company shall make a public communication or similar measure whereby the data subjects are informed in an equally effective manner of the breach.

## 2. Data Retention Policy

In order to comply with the requirement of the GDPR, the company will.

- annually assess and review the retention period of all personal data that it holds.

- consider the purpose or purposes that the company holds the information for as part of the process of deciding whether and for how long to retain it.

- securely delete information that is no longer needed for this purpose or these purposes; and

- update, archive or securely delete information if it goes out of date.

The current retention period for all personal data that the company holds is specified below:

- **Personal Data in relation to quotations not taken up by data subjects.**
  Retention Period: 1 year

  Retention Purpose: A client might take some time to consider whether to take up the quotation or not and the company needs to keep the client details to be able to serve them on quotations given out.

- **Personal Data in relation to quotations refused by the company.**
  Retention Period: 5 years

  Retention Purpose: As a measure to combat insurance fraud due to adverse KYC results to ensure that any rejected clients are not accepted.

- **Personal Data in relation to expired or lapsed insurance contracts**
  Retention Period: 10 years from the closure of all outstanding policy claims or policy maturity / surrender whichever comes last.

  Retention Purpose: Due to legal compliance and obligations arising from number of laws.

The retention periods indicated above do not relate to personal data which has been anonymised. Such anonymised data can be retained indefinitely.

Any deletion of data should be complete and therefore would include deletion of such personal data from any back-up systems.

# 15. PROCEDURES MANUAL

### A client exercising his / her right to be forgotten.

1. All such enquires must be directed in the first instance to the Data Protection Officer who will ensure that the company complies with the documented procedure and with the data subject's request. The DPO will keep records of all such requests from clients and shall be provided with any support that is required from any of the operational units within the company to fulfill any obligations under the GDPR.

2. As soon as a request from a data subject is received, this will be entered into the DPO Log and an acknowledgement must be sent to the client that his communication has been received and that the company will be reverting back shortly.

3. All requests from data subjects must be in writing and once these are received, the DPO must verify the data subject's identity before entertaining any such request. This can be done by asking for a copy of his / her identification on the understanding that this will be destroyed with any other documentation if the right to be forgotten request is deemed to be a valid request.

4. The DPO will ask the data subject whether he / she has any MWC Group products and if this is the case, the DPO will explain the consequence of exercising this right which might include the termination of any policies / investments held with any group company.

5. The DPO shall, where possible, try to establish the reason why the data subject has made this request. This will be done to establish the source for the request with the aim of putting into place any procedures to prevent this from this happening to other data subjects.

6. If the DPO establishes that the name of the data subject was on a referral list, the data subjects name must be deleted from this referral list and put into the Blacklist.

7. The DPO must establish how the name of the data subject was obtained to ensure that proper consent was obtained in the first instance OR that the name of the data subject was obtained from a publicly available source. The reason for this is to ensure that the data subjects name was obtained in accordance with the procedures established by the company. If the DPO determines that the data subjects name was obtained in any way that infringes the Company documented procedures, the Compliance Officer of the respective company will be advised.

8. As soon as the DPO is satisfied that the data subjects name has been deleted from any marketing lists and that the data subject has no policies through the MWC Group, the DPO will proceed to delete all information held on that data subject and ensure that the name is on the Blacklist of which an update is to be dispatched to all the TII Teams.

9. The DPO will them proceed to inform the data subject that the name has been deleted off marketing lists and that all policies have been cancelled (if applicable).

# APPENDIX 1 - PRIVACY POLICY

**MWC Group – Privacy Notice.**

**This is your guide to how your personal data is managed by MWC Group, please read it carefully.**

**Our commitment to privacy:**

Your information will be held by **MWC Group**, ("the **Company**").

We consider it crucial to protect your rights as our policyholder/s under applicable legislation and want you to feel confident about the privacy and security of your personal data.

## 1. The information we collect relating to you.

We collect and process various categories of personal information at the start of and for the duration of your relationship with us as per Section 3 below. We will limit the collection and processing of information to information necessary to achieve one or more legitimate purposes as identified in this Privacy Notice.

The information we collect about you may include:

- Basic personal information, including name and address, date of birth, nationality, country of birth and contact details.
- Financial information, including account and transactional information and history.
- Information about your family, lifestyle, social circumstances (such as dependents, marital status, next of kin and contact details).
- Details of any contact we have had with you such as any complaints or incidents.
- Information about how you use our products and services, such as insurance claims.
- Education and employment information, including salary.
- Results of checks relation to prevention of fraud and/or terrorist activities; and
- Information about how you use our website, including IP addresses or other device information.

We may also process certain special categories of information for specific and limited purposes, such as medical underwriting, detecting, and preventing financial crime or to make our services accessible to customers. We will only process special categories of information where we have obtained your explicit consent or we are otherwise permitted by law to do so (and then only for the particular purposes set out in Section *How we use your information',* for which the information is provided). This may include:

- Physical or psychological health details or medical conditions including genetic information and biometric information.
- Information about your race, ethnic origin, and religion; and
- Information about any prominent public function that you or your close associates previously or presently hold.

Where permitted by law, we may process information about criminal convictions or offences and alleged offences for specific and limited activities and purposes, such as to perform checks to prevent and detect crime and to comply with laws relating to money laundering, fraud, terrorist financing, bribery and corruption, and international sanctions.

If the data provided by you refer to third parties, you confirm to having obtained and received their prior consent to providing information on them, and to have informed them, before including them in our documentation.

**2. When and how we collect information about you.**

As you use our services, apply for products, make enquiries, and engage with us, information is gathered about you. We collect information about you in view of**:**

- Enquiries about our products which require your data and to provide you with quotations.
- The proper performance of your contract of insurance or the implementation of pre-contractual measures you request or require.
- Underwriting and issuing contracts of insurance, collecting premiums, and submitting other bills, settling claims, or paying other benefits, reinsurance, and actuarial activities.
- Compliance with legal obligations to which the Company is subject including but not limited to those obligations arising out of laws relating to money laundering, fraud, terrorist financing, bribery and corruption, and international sanctions.
- The establishing, exercising, or defending of any legal claims arising.
- Market research and analysis, internal management, accounting and auditing, product development and public relations.
- The exchange of information for preventing, suppressing, and detecting of insurance fraud and any other criminal activity which we are bound to report; and
- The protection and promotion of our legitimate interests and the proper conduct of our business.

Furthermore, we may receive personal or sensitive data relating to you and/or your dependents, spouse, partner, family from third parties such as Court Judgments database, the Registry of Company, World Check, fraud-detection and credit-reference agencies, doctors and health care professionals, hospitals, clinics and other health care providers and sources which are available to the public, which entities are all legally entitled to communicate such data and that such data is be processed for the stated purposes.

We may also record telephone conversations to offer additional security and resolve complaints. Personal data is also collected when you complete the "Contact Us" section on our website. Such personal data which is submitted online is then used by us in order to reply to your message. CCTV may be set up in our offices security purposes, if this is the case, these will be clearly indicated with appropriate signage once you enter our premises.

**3. How we use your information**

We have described the legal grounds for which your information may be used in detail below:

- Contractual necessity: its use is necessary in relation to a service or a contract that you have entered into or because you have asked for something to be done so you can enter into a contract with us. Please note that if you do not agree to provide us with the

requested information, it may not be possible for us to continue to provide products and services to you.
- Our legitimate interests: we may process your information where it is in our legitimate interests to do so, without prejudicing your interests or fundamental rights and freedoms. Its use is in accordance with our legitimate interests outlined in this Privacy Notice.
- Legal obligations: when you apply for a product or service (and throughout your relationship with us), we are required by law to collect and process certain personal information about you. Its use is necessary because of a legal obligation that applies to us (except an obligation imposed by a contract); and
- You have consented or explicitly consented to the using of your data (including sensitive data) in a specific manner.

All the necessary personal data that we shall collect will be held by us and processed:

- For consultancy and advisory services.
- For underwriting and internal risk assessment.
- Where you have specifically consented to doing so, to communicate with you market and promote our services and of those carefully selected third parties that MWC Group work with; and
- For any other purpose that may be necessary for the performance of the insurance and re-insurance service contract and/or for the execution of your instruction given to us from time to time or as may be allowed or required by any law or insurance regulation.

We may also engage in insurance industry standard profiling, wherein the assessment of risk is made by automated means. However, all final decisions which produce any legal effects on data subjects, including without limitation, the decision on whether to underwrite a risk and issue a contract of insurance, are taken with human intervention. We will keep such information as long as is necessary for the purpose(s) for which it was collected, such as underwriting, and in accordance with this Privacy Notice. Data will be securely destroyed when is no longer required.

## 4. Who we share your information with?

Whilst you are our customer, we undertake the responsibility not to transfer or exchange any information that we hold about you unnecessarily to or with any third parties without first obtaining your written consent. Nevertheless, and in line with our regulatory and legal obligations, there may be instances during the course of providing you with our services where we may be required to disclose, share, or exchange some or all of your personal information, whether sensitive or otherwise, to the following persons:

- Your introducers, your insurance intermediary, or brokers.
- Our agents and advisers who we use to help run your accounts and services.
- Our re-insurers or fund houses.
- Company in the MWC Group.
- Company that provides support services for the purposes of protecting our legitimate interests.
- Statutory and regulatory bodies, any public or governmental authority and/or to disclose any information before any court or adjudicating body of a competent jurisdiction where

such disclosure is compelled by law or authorised/ordered by a court or adjudicating body of a competent jurisdiction.
- In anonymised form, as part of statistics or other aggregated data shared with third parties.
- Company you ask us to share your data with; and
- Other insurances/investment Company/s as may be necessary.

**5. How long we hold your information.**

In line with our regulatory and legal obligations, including *inter alia* the Anti-Money Laundering regime and the Maltese Tax legislation, and for the purpose of underwriting and/or claims handling, we will keep your personal data, whether sensitive or otherwise, on the following basis:

- Our legal obligation for retention of your information.
- The term of the contractual relationship and necessary services to carry out such relationship; and
- Any request of the deletion of data by the relevant party, where applicable.

The information will be destroyed as soon as it is no longer required for the lawful purpose(s) for which it was obtained. We may on exception retain your information for longer periods, particularly where we need to withhold destruction or disposal based on an order from the courts or an investigation by law enforcement agencies or our regulators. This is intended to make sure that we will be able to produce records as evidence if they're needed. Nevertheless, data collected for inquiries which will not result in any type of contract will not be retained and will be discarded immediately.

**6. Implications of not sharing your information.**

As stated above, we may need to collect personal information by law, or under the terms of a contract we have with you.

If you choose not to give us this personal information, it may delay or prevent us from meeting our obligations. It may also mean that we may not be able to provide you with certain products and services that you request. We may not be able to continue to provide you with or renew existing products or services.

When we request information, we will tell you if providing it is a contractual requirement or not, and whether or not we need it to comply with our legal obligations.

**7. Processing your information outside the EEA**

Your information is stored on secure systems within the MWC Group premises and with providers of secure information storage. We may transfer or allow the transfer of information about you and your products and services with us to our service providers and other organisations outside the European Economic Area (the "EEA"), but only if they agree to act solely on our instructions and to protect your information to the same standards that are applied in the EEA.

We will only send your personal information outside of the EEA to:

- Follow your instructions.

- Comply with a legal duty; and
- Work with our service providers and advisors to help run your services.

If we do transfer information to our service providers and advisors outside of the EEA, we will make sure that it is protected in the same way as if it was being used in the EEA.

**8. Your rights**

**Providing and holding personal information comes with significant rights on your part and significant obligations on ours. You have several rights in relation to how we use your information:**

**The right to be informed -** You shall have the right to request us to inform you about the personal data that we process about you, the purpose of the processing, the categories of data that are being processed, the recipients of the data and the type of processing. If at any point you believe that the information, we process on you is incorrect then you can request to see this information, have a copy of such data and have it corrected or deleted. Any such access/ratification requests must be made to us in writing and must further be signed by you as the data subject.

If you later wish to raise a complaint on how we handled your personal data, you can contact us to have the matter investigated. In the event that you are not satisfied with our response or believe we are not processing your personal data in accordance with the law, you can then file a complaint with the Office of the Information and Data Protection Commissioner by accessing the following link: https://ico.org.uk/make-a-complaint/

**The right to maintain your personal data accurate and up to date -** We make every effort to ensure that all the personal data that we process about you is accurate and regularly updated. However, should you become aware of any errors or omissions in respect of your personal data you are kindly requested to inform us about such errors in writing. If it transpires that the information held is inaccurate, we will make the necessary amendments and inform you that these have been made.

**The right to be forgotten -** Where applicable, and in exceptional cases as allowed by law, you shall also have the right to request erasure of your personal data on *inter alia* the following grounds:

- Subject to our legal and regulatory obligation where processing is no longer necessary for its intended purpose.
- If your personal data has been given to us solely for consultation purposes, such as a life policy estimation, and you choose not to avail yourself of any of our services.
- When erasure is necessary for compliance with a legal obligation by the judiciary of Malta.
- When you object to the processing unless there are overriding legitimate grounds for us to process.
- When the data concerns a child and has been collected solely for marketing purposes and not arising out of a contractual relationship for services required from us.
- Where any data has been collected solely for marketing purposes.

Instead of requesting erasure, you can also request a restriction of the processing of data in cases where the personal data is inaccurate, unlawful, or pending a decision on a complaint lodged

by you. In such case we can only store your personal data and any further processing is only possible with your consent or in a limited number of situations.

**The right to data portability -** Since your personal data is subject to automated processing on the basis of our contractual relationship, you are thus allowed to request a copy of the data concerned in order for you to be able to transmit your processed data to another controller without any hindrance from our part.

**The right to object**- You have a right to object to us processing your personal information where the legal basis for our use of your data is our legitimate business interests or the performance of a task in the public interest. However, in doing so this may have an impact on the services and products we can/are willing to provide. You also have the right to object to the use of your personal data for direct marketing purposes. If you object to this use, we will stop using your data for direct marketing purposes.

**The right to withdraw your consent-** where we rely on your permission to process your personal information, you have a right to withdraw your consent at any time. We will always make it clear where we need your permission to undertake specific processing activities.

It is important to note that, in certain circumstances, you may not be able to exercise your rights as stipulated above or you may be able to exercise such rights but only in a limited manner, as dictated by law.

**9. How to contact us**

If you have any questions about how your personal data is gathered, stored, shared, or used, or if you wish to exercise any of your data rights, please contact our Data Protection Officer at:

**By email: dpo@mwcgroup.ch**

**By post: MWC Group UK** The Stables, Park Lidgett Farm Ossington, Newark, Nottinghamshire NG23 6LG

**10. Changes to this Notice**

We will update this Notice from time to time. Any changes will be communicated to you without delay, and where appropriate, notified to you by SMS or email.

**Conclusion:**

We undertake to implement all appropriate measures and safeguards in order to protect confidentiality, integrity and availability of all data processed. Accordingly, we declare that we have appropriate technical and organisational measures to protect your personal data against unauthorised or unlawful processing together with accidental alteration, destruction, loss and to also ensure compliance with the obligations imposed by the Data Protection legislation. We also maintain strict information security policies designed to prevent unauthorised access to your information by anyone, including our staff unless required to give a service. We can ensure you

that all of our staff who have access to any of the personal data held are personally responsible for maintaining customer confidentiality.

Nevertheless, kindly note that any duty of confidentiality owed by us is conditional on the representations and warranties made by you being true and complete in all respects and at all times and on the fulfilment by you of your obligations under the Application Documentation. We shall not be bound by any duty of confidentiality where disclosure is necessary, in our absolute discretion, to safeguard our legitimate interests.

# APPENDIX 2 – BREACH PROCESS