Home Comfort Retrofits

Your One Stop Shop for Cosy Living, Value and Service

Data Protection Policy

This Data Protection Policy sets out data protection requirements which must be complied with by anyone who processes personal data for, or on behalf of, Home Comfort Retrofits

Home Comfort Retrofits
The Enterprise Centre
The Harbour
Kilcock
Co Kildare
W23 A2T8

01 9125236
Info@homecomfortretrofits.ie
www.homecomfortretrofits.ie

1. Overview

Home Comfort Retrofits ('*HCR*', 'The Organisation'), as a contractor and provider of an energy retrofitting service for homeowners, processes personal data for a variety of purposes relating to its service users (or clients), employees, service providers and other third parties involved with the organisation. *HCR* is, therefore, a data controller and in some cases may act as a data processor. Consequent to this, *HCR* is subject to data protection legislation and regulation. This policy sets out data protection requirements which must be complied with by anyone who processes personal data for or on behalf of the organisation. *HCR* demands compliance with data protection law, from all of those with whom it interacts in the context of necessary personal data processing. Personal data processing for any stated lawful purpose must be necessary, proportionate and transparent.

2. Purpose

The purpose of this document is to provide a policy statement regarding the Data Protection obligations of *HCR*. This includes obligations in dealing with personal data, in order to ensure that *HCR* complies with the requirements of the relevant and applicable Data Protection Law (including the General Data Protection Regulation (EU Regulation 679/2016) (GDPR), Data Protection Act 2018, S.I. No. 336/2011 (Privacy and Electronic Communications) Regulations 2011).

3. Policy Objectives

The objectives of this policy are:

- to ensure *HCR* meets its statutory obligations under the GDPR and other relevant Data Protection Law;
- to inform data subjects (including service users of *HCR*, employees and other individuals whose personal data is being processed by *HCR*) as to how *HCR* manages its personal data and to inform them of their associated data protection rights under the GDPR and other relevant Data Protection Law;
- to ensure third-party service providers are aware of their legal obligations and responsibilities under the GDPR and other relevant Data Protection Law;
- to outline *HCR* requirements for arrangements with Joint Data Controllers, Independent Data Controllers and Processors;

- to advise any service providers for, or employees of, *HCR*, who may process personal data in the course of their duties, of their obligations under the GDPR and other relevant Data Protection Law;

4. Scope & Definitions

This Data Protection Policy applies to *HCR* and "third parties" (a natural person or legal entity other than *HCR* **-** but not the data subject) who process personal data for, on behalf-of, or in conjunction with *HCR*. This policy is concerned with personal data (including Special Category data) as defined by the GDPR.

Personal Data means any information relating to an identified or identifiable natural person, usually referred to as a '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.

Natural Person is a person (in legal meaning, i.e., one who has its own legal personality) that is an individual human being, as opposed to a legal person, which may be a private (i.e., business entity or non-governmental organisation) or public (i.e., governmental) organisation.

Processing means 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.

5. Data Protection Principles

The GDPR states that the protection of natural persons in relation to the processing of their personal data is a fundamental right. The principles of data protection apply to any personal data concerning an identified or identifiable natural person. Legislation requires that *HCR* or any third-party processing personal data for or on behalf of *HCR* must comply with these principles. The principles relating to processing of personal data are outlined below. (Note: Please refer to Appendix 1 - Glossary of Terms for common terms and definitions relating to data protection.) It has to be always borne in mind that while a processing operation involving personal data may have a lawful basis under the GDPR, it is possible the processing is still being done in breach of the data protection principles.

1. Personal data shall be:

(a) processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');

(b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes ('purpose limitation');

(c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');

(d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');

(e) 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 ('storage limitation'); and

(f) 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 ('integrity and confidentiality').

2. *HCR* or any third-party processing personal data for or on behalf of *HCR* is responsible for, and must be able to demonstrate, compliance with the principles as set out above. ('accountability')

5.1 Lawfulness

5.1.1 Legal bases for personal data processing.

The principle of lawfulness requires *HCR* to determine the legal basis for processing personal data prior to processing it. Personal data may only be processed if and to the extent that at least one of the following applies:

a) processing is necessary for the performance of a contract to which the data subject is party or to take steps at the request of the data subject prior to entering into a contract, e.g., performance of membership contract, performance of education contract, performance of designation contract;

b) the data subject has given consent to the processing of their personal data for one or more specific purposes;

c) processing is necessary for compliance with a legal obligation to which *HCR* is subject;

d) processing is necessary to protect the vital interests of the data subject or the vital interests of another natural person;

e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of an official authority vested in *HCR*;

f) processing is necessary for the purposes of the legitimate interests pursued by *HCR* 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.

The processing of personal data for purposes other than those for which the personal data were initially collected must only be undertaken where the processing is compatible with the purposes for which the personal data were initially collected. The basis for processing will be stated in our Privacy Notice on our website and shall be further recorded in Records of Processing Activities.

5.1.2 Consent

Where consent is required in order to process personal data, the consent must be sought and given by a clear, verifiable and affirmative action establishing a freely given, specific, informed and unambiguous indication of the data subject's agreement to the processing of personal data relating to them, such as by a written statement, including by electronic means, or an oral statement (if recorded). Note that silence, pre-ticked boxes or inactivity do not constitute consent.

5.1.3 Special Category Data

Personal data which are, by their nature, particularly sensitive in relation to fundamental rights and freedoms of individuals, merit specific protection as the context of their processing could create significant risks to an individual's fundamental rights and freedoms. Special category data include personal data relating to a natural person's:

- racial or ethnic origin;
- political opinions;
- religious or philosophical beliefs;
- trade union membership;
- genetics;
- biometrics;
- health; and
- sex life or sexual orientation.

Personal data falling under these categories can be processed only under specific conditions. Special category personal data **must not be processed** unless;

- the data subject has given explicit consent to the processing of those personal data for one or more specified purposes;
- processing is necessary for the purposes of carrying out the obligations and exercising specific rights of *HCR* or of the data subject in the field of employment and social security and social protection law;
- 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;
- processing relates to personal data which are manifestly made public by the data subject;
- processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;
- processing is necessary for reasons of substantial public interest;
- processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services or pursuant to contract with a health professional;
- processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices;
- processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes. Suitable and specific measures, including security measures, must be applied in respect of processing special category data.

5.1.4 Cookies

Cookies are small items of code placed on a user's computer by a website and are vital to the functioning of modern internet sites. Cookies allow website operators to determine how users browse their sites and are a technical pre-requisite for some applications.

Data protection legislation/regulation applies to the use of cookies and other similar technologies where it involves the processing of personal data. The 'ePrivacy Regulation' (S.I. 336/2011) is also applicable to certain types of data processing, including the use of cookies and similar technologies. Consent of the data subject must be obtained to use cookies. Data

subjects must be provided with certain easily accessible, 'clear and comprehensive' information on the technology being used and the purpose(s) for which it is used.

Note: Once *HCR* has its website up and running a Privacy Notice and Cookie Notice will be available.

5.2 Fairness and Transparency

The principles of fairness and transparency require *HCR* to provide the data subject with information necessary to ensure fair and transparent processing, taking into account the specific circumstances and context in which the personal data are processed.

HCR or any third-party processing personal data for or on behalf of *HCR*, will treat the data subject fairly by using their personal data for purposes and in a way they would reasonably expect and will ensure that their personal data is not used for a different purpose other than that which the individual agreed to or would reasonably expect. *HCR* commits to use personal data only for the purposes for which it was collected. If in the future this ever changes and *HCR* intends to further process personal data for a purpose other than that for which it was collected, *HCR* as controller will provide the data subject prior to that further processing with information on that other purpose and with all relevant information as laid out under Art.13.3 GDPR.

HCR will advise the data subject of the identity of the data controller, the existence of the personal data processing operation, the purpose of processing, and of their rights as a data subject. The communication relating to the processing of personal data will be easily accessible and easy to understand, and the language used will be clear and plain.

In this regard, *HCR* will provide the data subject with all information providing the data subject with a detailed and clear explanation of how *HCR* will manage their personal data, at the point of data collection, including electronic or hard copy forms, and including collection through information technology systems.

Where personal data is obtained from another source, in accordance with Art.14 GDPR further information will be provided:

- within one month at the latest after obtaining the personal data;
- if personal data are to be used to communicate with the data subject, at the latest at the time of the first communication with the data subjects;
- if disclosure to another recipient is envisaged, at the latest when personal data is first disclosed. Note that the data subject will be informed of the existence and consequences of profiling, i.e., 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, e.g., personal preferences, interests, reliability, behaviour.

5.3 Purpose Limitation

The principle of purpose limitation requires *HCR* to collect personal data only for a specified, explicit, and legitimate purpose and to not further process the data in a manner that is incompatible with those purposes. *HCR* will determine the specific purposes for which personal data are processed which will be explicit and legitimate and determined prior to the collection of the personal data.

5.4 Data Minimisation

The principle of data minimisation requires *HCR* to ensure that personal data is adequate, relevant and limited to what is necessary for the purposes for which they are processed. *HCR* or any third party processing personal data for or on behalf of *HCR* will not collect personal data that is not strictly necessary for the purpose for which it is collected. Processing activities must be managed to ensure that personal data continues to be adequate, relevant, and not excessive. Personal data must be processed only if the purpose of the processing could not reasonably be fulfilled by other means. Data Minimisation requires that the period for which the personal data are stored is limited to a strict minimum (see also the principle of 'Storage Limitation' below).

5.5 Accuracy

The principle of accuracy requires *HCR* to ensure that personal data are accurate and, where necessary, kept up to date; taking every reasonable step to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay. A data subject will be asked to confirm the accuracy at the point of collection of personal data and also to notify *HCR* of any changes in personal data to enable *HCR* to update records accordingly. *HCR* will also be proactive and verify the accuracy of personal data on a regular basis.

5.6 Storage Limitation

The principle of storage limitation requires that *HCR* store personal data only in a form which permits identification of data subjects for as long as is necessary for the purposes for which the personal data are processed. It also requires that the period for which personal data are stored is limited to a strict minimum. In order to ensure that the personal data are not retained longer

than necessary, *HCR* will establish and manage specific retention periods for storage of the different categories and types of personal data, i.e. Where exact periods can not be definitely outlined the criteria used to determine the retention period will be communicated to the data subject. Any retention periods mandated by law, such as Revenue Law, will be strictly followed. *HCR* may retain personal data for longer periods if the data will be processed solely for statistical purposes, subject to the implementation of appropriate technical and organisational measures to safeguard the rights and freedoms of the data subject.

5.7 Integrity and Confidentiality (Data Security)

The principle of integrity and confidentiality requires *HCR* or any third-party processing personal data for or on behalf of *HCR*, to process personal data in a manner that ensures its integrity and confidentiality. This must encompass the availability and security of personal data, including preventing unauthorised access to or use of personal data and also to protect against unauthorised alteration, destruction, damage or loss, using appropriate technical or organisational measures.

HCR or any third-party processing personal data for or on behalf of *HCR*, must evaluate the risks inherent in the processing and implement measures to mitigate those risks, such as encryption. Consideration must be given to the risks that are presented by personal data processing, such as accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed which may in particular lead to physical, material or non-material damage.

Taking into account the state of the art, (e.g., technological developments) the costs of implementation and the nature, scope, context and purposes of processing, as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, all parties to an arrangement/agreement/contract must implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including:

(a) anonymisation* where possible;
(b) the pseudonymisation* and encryption of personal data;
(c) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
(d) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;

(e) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing. * For further information on anonymisation and pseudonymisation, refer to Appendix 3.

5.8 Accountability

HCR or any third-party processing personal data for or on behalf of *HCR* is responsible for and must be able to demonstrate compliance with the principles of data protection to stakeholders, in particular to Supervisory Authorities, i.e., the independent public bodies charged with responsibility for data protection in each member state of the EU. The Supervisory Authority in Ireland is the Data Protection Commission.

In order to demonstrate compliance, *HCR* or any third-party processing personal data for or on behalf of *HCR*, must have appropriate technical and organisational measures in place. Such measures may include some or all of the following depending on legal requirements: policies and procedures; records of processing activities (ROPAs); data protection notices; 'privacy by design' and 'privacy by default' assessments, legitimate interest assessments (LIAs), data protection impact assessments (DPIAs), transfer impact assessments (TIAs); appropriate technical and organisations controls.

HCR or any third-party processing personal data for or on behalf of *HCR* is obliged to cooperate with the Supervisory Authority and to make Records of Processing Activities available to it on request.

5.8.1 Records of Processing Activities (ROPAs)

While *HCR* is processing personal data in its capacity as a data controller (or any third-party processing personal data for or on behalf of *HCR*,) it will maintain records of processing activities (ROPAs) to demonstrate accountability for compliance with data protection legislation/regulation. This currently is not mandatory for *HCR* under Art. 30.5 GDPR but nevertheless *HCR* will maintain these records.

ROPAs are compiled in a central register of processing activities. The register must document at a minimum:

- the name and contact details of the controller, i.e., *HCR* and, where applicable, any joint controllers, and the Data Protection Officer;
- the purposes of the processing;
- a description of the categories of data subjects e.g., service users, employees etc.;
- a description of the categories of personal data, e.g., contact details, age, date of birth etc.;

- the categories of recipients to whom the personal data have been or will be disclosed including recipients outside the EEA or to international organisations, e.g. statutory authorities where legally obliged, admin staff, auditors, book-keepers etc.;
- where applicable, transfers of personal data outside the EEA or to an international organisation, including the identification of that country or international organisation and, in such cases the relevant safeguards applied, e.g., standard contractual clauses when transferring personal data to UK, India, US etc.;
- the envisaged time limits for erasure of the different categories of data;
- a general description of the technical and organisational security measures, e.g., encryption of personal data.

HCR or any third-party processing personal data for or on behalf of *HCR*, must maintain ROPAs for activities where it/they acts/act as a *data processor*. The records must, at a minimum, contain the following information:

- the name and contact details of each data controller on behalf of whom the data processor is acting, and where applicable, the controller's representation or DPO;
- the categories of processing carried out on behalf of each data controller;
- 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, in such cases the relevant safeguards applied;
- a general description of the technical and organisational security measures.

5.8.2 Training and Awareness

HCR provides data protection training to ensure employees are aware of their respective obligations under data protection legislation/regulation which covers the key requirements of data protection legislation/regulation, e.g., data protection principles, data subject rights, sharing/transferring of personal data, data breach management, and security of personal data.

6. Data Subjects' Rights & Complaints

6.1 Subject Rights

Data protection legislation/regulations confer the following rights on data subjects:

1. Right to access;
2. Right to rectification;
3. Right to erasure ("right to be forgotten");
4. Right to restriction of processing;

5. Right to data portability;
6. Right to object (to processing); and
7. Rights in relation to automated decision-making, including profiling.

6.1.1 Right to Access

A data subject(s) has the right of access to their personal data processed by *HCR*, or any third-party processing personal data for or on behalf of *HCR*, and to exercise that right easily and at reasonable intervals, in order to be aware of, and verify, the lawfulness of the processing.

6.1.2 Right to Rectification.

A data subject has the right to obtain from *HCR*, or any third-party processing personal data for or on behalf of *HCR*, without undue delay the rectification of inaccurate personal data concerning them. Taking into account the purposes of the processing, the data subject has the right to have incomplete personal data completed, including by means of providing a supplementary statement.

6.1.3 Right to Erasure (also known as the Right to be forgotten)

A data subject has the right to obtain from *HCR*, or any third-party processing personal data for or on behalf of *HCR*, the erasure of personal data concerning them without undue delay where one of the following grounds applies:

a) the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;
b) the data subject withdraws consent on which the processing is based, and where there are no other legal grounds for the processing;
c) the data subject objects to the processing (and that processing is based on the performance of a task carried out in the public interest or processing is based on legitimate interest) and there are no other overriding legitimate grounds for the processing, or the data subject objects to the processing for direct marketing purposes, including profiling (refer the Right to Object also);
d) the personal data have been unlawfully processed;
e) the personal data have to be erased for compliance with a legal obligation in EU or Member State law to which the controller is subject;
f) the personal data have been collected in relation to the offer of information society services to the data subject as a child.

HCR, or any third-party processing personal data for or on behalf of *HCR*, must anonymise and/or pseudonymise personal data where possible rather than erase if:

- erasure is prohibited by legislation/regulation;
- erasure would impair the legitimate interests of the data subject;
- erasure is not possible without disproportionate effort due to the specific type of storage; or
- where the data subject has disputed the accuracy of the personal data, and *HCR* disagrees with that assertion and resolution has not been reached.

6.1.4 Right to Restriction (of processing)

A data subject(s) has the right to obtain from *HCR*, or any third-party processing personal data for or on behalf of *HCR*, restriction of processing where one or more of the following applies:

1 the accuracy of the personal data is contested by the data subject, for a period enabling *HCR*, or any third-party processing personal data for or on behalf of *HCR*, to verify the accuracy of the personal data;

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

3 *HCR*, or any third-party processing personal data for or on behalf of *HCR*, 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 defence of legal claims;

4 the data subject has objected to processing pending the verification of whether the legitimate grounds of *HCR*, or any third-party processing personal data for or on behalf of *HCR*, override those of the data subject.

Where processing has been restricted, the personal data must, with the exception of storage, only be processed with the data subject's consent or for the establishment, exercise or defence of legal claims or for the protection of the rights of another natural or legal person or for reasons of important public interest of the EU or a Member State.

6.1.5 Right to Portability

A data subject has a right to receive personal data concerning them which they have provided to *HCR* or any third-party processing personal data for or on behalf of *HCR*, in a structured, commonly used, machine-readable format and has the right to transmit those data to another controller without hindrance from *HCR* or any third-party processing personal data for or on behalf of *HCR*, where:

1. the processing is based on consent or the performance of a contract; and
2. the processing is carried out by automated means.

The data subject has the right to have the personal data transmitted directly from one controller to another, where technically feasible.

6.1.6 Right to Object

The data subject has the right to object at any time, to processing of personal data concerning them where the processing is necessary based on legitimate interests pursued by a controller (Art.6.1 (e) GDPR or performance of a task in the public interest/exercise of official authority , Art.6.1 (f) GDPR and including profiling based on those provisions (Art. 21.1 GDPR)

If either of these legal bases are used by *HCR*, then *HCR* must inform individuals of their right to object "at the point of first communication" and in the *HCR* Data Privacy Notice. This must be explicitly brought to the attention of the data subject and presented clearly and separately from any other information.

HCR or any third-party processing personal data for or on behalf of *HCR* will no longer process the personal data unless it can demonstrate 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.

Where personal data are processed for direct marketing purposes, the data subject has the right to object at any time to processing of personal data concerning them for such marketing, which includes profiling, to the extent that it is related to such direct marketing.

Where the data subject objects to such processing, the personal data must no longer be processed for such purposes. Where personal data are processed for historical research purposes or statistical purposes, the data subject, on grounds relating to their particular situation, has the right to object to processing of personal data concerning them, unless the processing is necessary for the performance of a task carried out for reasons of public interest.

Note where processing is based on consent, and there is no other justification for processing, e.g., performance of contract or legal obligation, the request should be upheld. However, before excluding the data subject's personal data from processing, it must be confirmed that consent is indeed the only basis for the processing.

6.1.7 Rights in relation to automated decision-making, including profiling.

The data subject(s) has the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning them or similarly significantly affects them.

This right does not apply if the decision:

1 is necessary for entering into, or performance of, a contract between the data subject and a data controller;

2 is authorised by EU or Member State law to which *HCR* is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or

3 is based on the data subject's explicit consent.

Note that additional consideration is required if the data is special category data. Processing which involves automated decision-making, including profiling, must cease immediately upon receipt of an objection to such processing, unless there are "compelling" legitimate grounds for the processing, i.e., necessary for performance of a contract, or if processing is for the establishment, exercise or defence of legal claims.

In cases 1 and 3 above, *HCR* will implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, at least the right to obtain human intervention on the part of *HCR*, to express their point of view, and to contest the decision. Note that additional consideration is required if the data is special category data. Processing which involves automated decision-making, including profiling, must cease immediately upon receipt of an objection to such processing, unless there are "compelling" legitimate grounds for the processing, i.e., necessary for performance of a contract, or if processing is for the establishment, exercise or defence of legal claims.

6.2 Data Protection Complaints.

Any questions about how personal data is processed and/or complaints about the use of personal information should be emailed to:

info@homecomfortretrofits.ie

or Post to: Home Comfort Retrofits, Enterprise Centre, Kilcock, Co. Kildare.W23 A2T8.

If the issue cannot be resolved satisfactorily through consultation between the Data Subject and *HCR*, then the Data Subject may refer the complaint to the Supervisory Authority.

7. Data Protection - Technical and Organisational Methods

7.1 Data Protection by Design

HCR applies appropriate technical and organisational methods, e.g., pseudonymisation, which are designed to comply with the data protection principles, such as data minimisation, and integrate the necessary safeguards into processing activities in order to meet the requirements of data protection legislation/regulation, and to protect the rights of data subjects. This is done by design both at time of determination of the means of processing and throughout the processing operation.

"Data Protection by Design" requires that *HCR* consider data protection requirements when considering any action which involves the processing of personal data e.g., product/service development/promotion/ delivery, internal projects, IT systems and/or software development, etc.

In practice, this means that *HCR* will ensure that data protection is taken into consideration for all business processes and systems which involve personal data processing activities from the design/inception stage right through the lifecycle of such processes and systems. Note that data protection by design does not just refer to the design of systems, products and services, it also refers to organisational policies and processes, and business practices which have data protection implications. The Software to be used is specifically designed for the One Stop Shop Business model by BCR Comply and their Privacy Policy is available here.

7.2 Data Protection by Default

HCR implements appropriate technical and organisational measures to ensure that by default, only personal data necessary for each specific processing purpose is processed. This applies to:

- the amount of data collected;
- the extent of the processing;
- the period of storage;
- accessibility.

In particular, the measures need to ensure that by default, the data is not made accessible to an indefinite number of people without the intervention of the data subject.

"Data Protection by Default" requires that once a product or service has been released, the strictest data protection settings should apply by default, without any manual input from the end user. In addition, any personal data provided by a user to enable optimal use of a product or service should only be kept for the amount of time necessary to provide the product or service.

HCR will ensure appropriate technical and organisational measures are implemented by design and by default, providing a level of protection appropriate to the risk, taking account of the state of the art (e.g., technological developments relating to IT security), the costs of implementation, and the nature, scope, context and purposes of processing, as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons.

Note an approved certification mechanism may be used as an element to demonstrate compliance with the requirements. Data Protection by Design and by Default essentially mean that *HCR* will integrate or "bake in" data protection into processing activities and business practices from the design stage right through the lifecycle as a legal/regulatory requirement. This involves assessing and considering each processing activity on a case-by-case basis.

7.3 Data Protection Impact Assessment (DPIA)

HCR will, prior to processing personal data, carry out a Data Protection Impact Assessment (DPIA) of the envisaged processing activity, where the type of processing, in particular processing 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. A DPIA is a process to help identify and minimise the data protection risks of a new project or changes to existing processes (operational or technical) which may introduce, or increase, significant risk to the security of the personal data to be processed. A single assessment may address a set of similar processing operations that present similar risks.

A DPIA must be undertaken in the case of:

- processing personal data on a large scale;
- innovative use or application of technological or organisation solutions, e.g., face recognition for access;
- a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person;
- processing of special category data, or of personal data relating to criminal convictions and offences;
- personal data sets which have been matched or combined; (for example originating from two or more data processing operations performed for different purposes and/or by different data controllers in a way that would exceed the reasonable expectations of the data subject);

- personal data concerning vulnerable data subjects e.g., personal data of children;
- a systematic monitoring of a publicly accessible area on a large scale, e.g., CCTV;
- data sharing/transfer across borders outside the EU;
- when processing in itself "prevents data subjects from exercising a right or using a service or a contract" e.g., where customers are screened against a credit data base for loan approval.

A DPIA must contain at minimum:

- a systematic description of the envisaged processing activity and the purposes of the processing, including, where applicable, the legitimate interest pursued by *HCR*;
- an assessment of the necessity and proportionality of the processing activity in relation to the purposes;
- an assessment of the risks to the rights and freedoms of data subjects; and
- the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance legislation/regulation taking into account the rights and legitimate interests of data subjects and other persons concerned.

Appropriate controls must be selected and applied to reduce the level of risk associated with processing individual personal data to an acceptable level, by reference to the requirements of data protection legislation/regulations.

Note that compliance with approved codes of conduct may be considered when assessing the impact of the processing operation undertaken by *HCR* for the purposes of the DPIA.

The DPO or a qualified designated person either internal or external must be engaged when undertaking a DPIA.

If the conclusion of the DPIA is that, despite mitigants to reduce the risks to individuals, a high residual risk remains, the Supervisory Authority must be consulted for approval to proceed before implementing the process.

8. Personal Data Sharing/Transfer

HCR shares data, i.e., makes data available and receives data, including personal data, to support the proper functioning of the organisation in compliance with applicable legislation and regulations. Data may be shared with third parties including, but not limited to, service providers, IT system/service providers, partners and others where there is a legal obligation to do so. Note that the sharing of personal data must only be undertaken where no other means are available to achieve the required outcome, except where *HCR* is legally compelled to share.

The process of sharing data will require the transfer of data, i.e., the transmission of data or otherwise from one location to another location. It may also include the publication of data, e.g., making data accessible on a shared portal or website.

A key objective when sharing data is to maintain its confidentiality and integrity, and to minimise the risk of unauthorised or unlawful processing, accidental loss, unauthorised disclosure, damage or destruction.

Where sharing of personal data is deemed necessary, an assessment of the process and relevant procedures must be undertaken to confirm the nature of any third-party relationships and the relevant arrangements/agreements/contracts.

A third-party with whom *HCR* intends to share data, will be identified as either:

1 a third-party processor, e.g. IT service providers;

2 a data controller:

2.1 a joint data controller, e.g., certain partners;

3 an independent or separate data controller, (e.g., SEAI)

A formal written and signed arrangement/agreement/contract, normally referred to as DPA, depending on the nature of the relationship, setting out each party's obligations for compliance with data protection legislation/regulation, and containing the appropriate data protection clauses, will be in place prior to sharing any personal data with a third-party processor or a joint data controller.

The requirements for a formal written arrangement with independent data controllers will be assessed on a case-by-case basis. The requirements will be based on the nature, volume and frequency of data to be shared. For example, a special arrangement with the SEAI will be in place for the purposes of the One Stop Shop Grant Scheme.

All parties to a data sharing arrangement/agreement/contract must take appropriate steps to ensure that any natural person acting under their authority who has access to personal data does not process them except on their instructions unless he or she is independently required to do so by EU or Member State law.

HCR will only engage with a third-party who can provide 'sufficient guarantees' to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of data protection legislation/regulation and ensure the protection of the rights of the data subject(s). Adherence to an approved code of conduct or an approved certification mechanism, e.g., ISO 27001, by a third-party may be used by *HCR* as an element by which to demonstrate sufficient guarantees.

9. Third-Party Risk Management

9.1 Third-Party Processors

A third-party service provider is any individual or organisation contracted by *HCR* to provide goods and/or services, e.g. I.T. systems/services, project management, records storage. Third-party service providers who process data including personal data on behalf of *HCR* are "third-party processors".

All processing by a third-party processor on behalf of *HCR* must be governed by a clear and comprehensive contract under EU or Member State law, that is binding on the processor with regard to *HCR*, 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 *HCR*.

The contract must stipulate, in particular, that the processor:

a. will process the personal data only on the documented instructions of *HCR*, including with regard to transfers of personal data to a third country or an international organisation, unless required to do so by EU or Member State law to which the processor is subject; in such a case, the processor must inform *HCR* of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest;

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

c. takes all measures required pursuant to GDPR Article 32 relating to security of processing;

d. respects conditions referred to under GDPR Article 28 for engaging another processor;

e. taking into account the nature of the processing, assists *HCR* by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of *HCR*s obligation to respond to requests for exercising the data subject's rights;

f. assists *HCR* in ensuring compliance with the obligations pursuant to Articles 32 to 36, taking into account the nature of processing and the information available to the processor;

g. at the choice of *HCR*, deletes or returns all the personal data to *HCR* after the end of the provision of services relating to processing, and deletes existing copies unless EU or Member State law requires storage of the personal data;

h. makes available to *HCR*, as controller, all information necessary to demonstrate compliance with data protection obligations and allow for and contribute to audits, including inspections, conducted by *HCR* or an auditor mandated by *HCR*;

i. must notify *HCR* immediately after becoming aware of any 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 and provide *HCR* with such co-operation and assistance as may be required to mitigate against the effects of, and comply with any reporting obligations which may apply in respect of, any such breach.

With regard to point (h) above, the processor must immediately inform *HCR* if, in its opinion, an instruction infringes data protection legislation/regulation or other EU or Member State data protection provisions.

In all circumstances, where the processing of personal data is contracted to a third-party processor including, for example to a 'cloud computing' service provider, the third-party processor must protect personal data through sufficient technical and organisational security measures and take all reasonable compliance steps to ensure the security of the data.

HCR as the data controller is responsible for defining each party's obligations for compliance with data protection legislation/regulation. All contracts relating to data processing will be reviewed to ensure *HCR* can meet all of the requirements of the contract and that *HCR* is only accepting the appropriate level of liability.

Processors are legally obliged not to engage another processor, i.e., a sub-processor, without prior specific written authorisation of *HCR*, and to inform *HCR* of any intended changes concerning the addition or replacement of other processors, thereby giving *HCR* the opportunity to object to such changes if deemed necessary.

Where a processor engages a sub-processor to carry out specific processing activities on behalf of *HCR*, the same data protection obligations as set out in the contract between *HCR* and the processor must be imposed on the sub-processor by way of a contract under EU 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 data protection legislation/regulation. Where the sub-processor fails to fulfil its data protection obligations, the initial processor must remain fully liable to *HCR* for the performance of the sub processor's obligations.

Note the processor, and any person acting under the authority of *HCR* or the processor, who has access to personal data, must not process those data, except on instructions from *HCR* as controller, unless required to do so by EU or Member State law.

If a processor determines the purposes and means of processing, the processor may then be considered to be a controller in respect of that processing.

HCR may also act as a third-party processor in some circumstances. When acting as a processor, *HCR* will comply with relevant data protection legislation/regulations in this regard. These include ensuring that the data processed by *HCR* on behalf of the relevant data controller is subject to appropriate technical and organisational measures to ensure a level of security appropriate to the risk, and ensuring the processing is governed by a contract which includes the appropriate provisions of data protection legislation/regulation.

9.2 Data Controllers

A Data Controller means the natural or legal person, public authority, agency or other body which, alone (independent controller) or jointly with others (joint controllers), determines the purposes and means of the processing of personal data. Where two or more controllers jointly determine the purposes and means of processing, they are deemed to be joint controllers. All controllers (independent or joint) must comply with Data Protection legislation/regulation in their own right.

9.2.1 Joint Controllers

HCR acts as a joint controller of personal data where *HCR* together with other entities determine the purposes and means of the relevant processing. In such circumstances "the essence" (Article 26, GDPR) of the arrangement between *HCR* and the other joint controller(s) must be made known to the data subject in a transparent manner, e.g., through the Data Privacy Notice or more often referred to as a Privacy Notice. These should be available on the *HCR* website. ?????

HCR, along with the other joint controllers with whom *HCR* shares personal data, must determine and document (in the arrangement), the respective roles and responsibilities of each party for compliance with data protection legislation/regulations, and in particular, regarding the rights of the data subject and their respective duties relating to data collection.

All arrangements must designate a point-of-contact of the lead controller for data subjects. Note that, irrespective of any arrangement between joint controllers, a data subject may exercise their rights in respect of and against any or all of the controllers.

All arrangements relating to data processing will be reviewed to ensure the requirements of the arrangement can be met and that *HCR* is only accepting an appropriate level of liability.

9.2.2 Independent/Separate Data Controllers

Where information is intended to be shared between two parties, and each party is acting as an independent data controller in their own right, i.e., there is neither a processor nor joint

controller relationship, then depending on the nature and context of the information to be transferred, appropriate controls must be put in place to protect the rights of the data subject.

Where personal data is to be shared between two independent controllers and sharing is taking place using legitimate interest as the legal basis, a legitimate interest assessment will be undertaken prior to the sharing of any personal data to ensure the fundamental rights and freedoms of the data subjects are protected.

Where the data is to be shared between the two independent controllers on a legitimate interest basis, an appropriate data transfer agreement will be put in place which specifies the obligations of both parties.

The data transfer agreement should include the following clauses with each party agreeing that:

- it will comply with its obligations under data protection legislation/regulations in relation to any transferred personal data;
- each will act as a separate controller in respect of shared personal data and that neither will process such personal data on behalf of the other;
- it will take all steps necessary to be able to provide relevant personal data to the other party in compliance with its obligations under data protection legislation/regulations, including but not limited to ensuring that it has provided such information to and, to the extent necessary, obtained such consents from, the relevant data subjects as is necessary under data protection legislation/regulations to enable lawful transfer of personal data to the other party;
- it will notify the other party promptly upon becoming aware of any data subject request or complaint or any correspondence or action by any competent data protection authority in respect of the provision of any personal data to the other party or receipt of any personal data from the other party and will provide the other party with such cooperation and assistance as may be reasonably required for the other party to comply with its obligations under data protection legislation/regulations in respect of any such request, complaint, correspondence or action;
- it will notify the other party immediately after becoming aware of any 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 and provide the other party with such cooperation and assistance as may be required to mitigate against the effects of, and comply with any reporting obligations which may apply in respect of, any such breach.

- it will provide the other party with such cooperation and assistance as may be reasonably required for the other party to comply with the other party's notification obligations as a controller under data protection legislation/regulations in respect of obtaining any personal data, including by delivering any notice provided to it by the other party to the relevant data subjects of such personal data;
- where the transfer of any personal data between the parties involves a transfer of such personal data to a territory outside the European Economic Area that has not been recognised by the European Commission as ensuring an adequate level of protection pursuant to Data Protection Law, the parties must ensure that the transfer is conducted in compliance with applicable requirements under data protection legislation/regulations which may include by entering into standard contractual clauses (controller to controller) approved for this purpose by the European Commission (refer also section on International Data Transfers below).

10. International Data Transfers

Data protection legislation/regulations impose restrictions on the transfer of personal data, or making personal data available to another third-party, outside the European Economic Area (EEA - European Union countries and Norway, Iceland and Liechtenstein), unless the rights of the individuals in respect of their personal data is protected in another way, or one of a limited number of exceptions. Any country outside the EEA is referred to as a "third country". Restrictions are in place to ensure that the level of protection of individuals afforded by EU data protection legislation and regulations is not undermined.

Personal data cannot be transferred to a third country without one of the following provisions:

10.1 Transfers based on an "Adequacy Decision"

The first thing to consider when transferring personal data to a third country is if there is an "adequacy decision". An adequacy decision means that the European Commission has decided that a third country or an international organisation ensures an adequate level of data protection. The effect of such a decision is that personal data can flow from the EEA to that third country without any further safeguard being necessary. In other words, the transfer is the same as if was carried out within the EU. Refer to Appendix 4 for more details on third countries with whom adequacy decisions are in place (or partially in place).

10.2 Transfers subject to "Appropriate Safeguards"

In the absence of an adequacy decision, a transfer may be made if the controller or processor has provided "appropriate safeguards". These safeguards may include:

- Standard Contractual Clauses: These are model data protection clauses that have been approved by the European Commission and enable the free flow of personal data when embedded in an arrangement/agreement/contract. The clauses contain contractual obligations on the "data exporter" and the "data importer" and rights for the individuals whose personal data is transferred. Individuals can directly enforce their rights against the data exporter and the data importer. There are two sets of standard contractual clauses for restricted transfers between a controller and controller, and one set between a controller and processor.
- Binding corporate rules (BCRs): BCRs form a legally binding internal code of conduct operating within a multinational group, which transfers personal data from the group's EEA entities to the group's non-EEA entities.
- Approved codes of conduct: Under specific circumstances, codes of conduct may be considered an appropriate safeguard. Codes are voluntary and set out specific data protection rules for categories of controllers and processors.
- Approved certification mechanisms: Certification is defined by the ISO as "the provision by an independent body of written assurance, e.g., a certificate, that the product, service or system in question meets specific requirements". Certification mechanisms may be developed to demonstrate the existence of appropriate safeguards provided by controllers and processors in third countries.

10.2.1 Transfer Impact Assessments

A Transfer Impact Assessment (TIA) must be completed for international data transfers to a "third country" (where no "adequacy decision" has been granted by the European Commission to that country relating to the nature of the transfer taking place). The TIA must take into consideration whether essential guarantees are adequate and whether supplementary measures must be put in place to enable the transfer to take place. The controller or processor must document the assessment as well as the suitable safeguards.

10.3 Derogations for specific situations

Derogations are exemptions from the general principle that personal data may only be transferred to a third country if an adequate level of protection is provided for in that third

country. A data exporter should first endeavour to frame transfers with one of the mechanisms guaranteeing adequate safeguards listed above, and only in their absence use the available derogations.

11. Personal Data Breach Management

A 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.

HCR has procedures for managing any personal data breach to ensure that the rights and freedoms of data subjects are upheld. The agreed procedures for managing data breaches will be followed in all instances to ensure compliance with legislation/regulation.

The procedures incorporate the following policy requirements:

- Any known or suspected breach of personal data must be reported by *HCR* employees to the *HCR* Data Protection Officer.
- Joint-Controllers/Third-Party Processors must notify *HCR* immediately after becoming aware of any 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 and provide *HCR* with such co-operation and assistance as may be required to mitigate against the effects of, and comply with any reporting obligations which may apply in respect of, any such breach.
- *HCR* will notify data subject(s) of a personal data breach without undue delay, where the breach is likely to result in a high risk to the rights and freedoms of the natural person, in order to allow the data subject(s) to take the necessary precautions.
- *HCR* will notify the appropriate Supervisory Authority of a personal data breach without undue delay and, where feasible, not later than 72 hours after having become aware of it, unless *HCR* is able to demonstrate, in accordance with the accountability principle, that the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the Supervisory Authority is not made within 72 hours, the reasons for the delay will be explained when reporting.

12. Responsibilities

12.1 Data Protection Governance

HCR is committed to protecting the privacy and rights of individuals in compliance with data protection legislation and regulations. *HCR* is currently examining the establishment of a Data

Protection Management Framework. This Framework will be overseen and maintained by a Senior Management Steering Group to provide structure for the development, implementation, management, monitoring and reporting of appropriate activities to meet this commitment. The Framework will include appropriate technical and organisational measures, e.g., policies, procedures, training, operational and technical safeguards, and other mechanisms, to provide direction, raise awareness, establish controls and mitigate internal and external risks. Operational execution of data protection management activities will be carried out by a Data Protection Working Group, made up of senior management and the DPO.

The primary responsibilities of members of the *HCR* Senior Management Steering Group will be to maintain governance and oversight of the Data Protection Management Framework in *HCR*. Members of the Data Protection Working Group will have the responsibility to operationalise and monitor the management activities within the Data Protection Management Framework.

12.2 Employees

All *HCR* employees must comply with *HCR*'s Data Protection Policy and associated policies when processing personal data. All employees must undertake mandatory data protection training as required by *HCR*.

12.3 Heads of Department/Management

Heads of Department are responsible for compliance with *HCR*'s Data Protection Policy and associated policies and the implementation, management and monitoring of related procedures for their respective areas of responsibility.

12.4 Data Protection Officer (DPO)

HCR has appointed a Data Protection Officer (DPO). It is the responsibility of the DPO:

- to inform and advise *HCR* and the employees who carry out processing of their obligations pursuant to the GDPR and to Irish data protection provisions;
- to monitor compliance with the GDPR, with Irish data protection provisions and with the policies of *HCR* in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits;
- to provide advice where requested as regards the data protection impact assessment and monitor its performance pursuant to Article 35 (GDPR);
- to cooperate with the supervisory authority;

- to act as the contact point for the supervisory authority on issues relating to processing, including the prior consultation referred to in Article 36 (GDPR), and to consult, where appropriate, with regard to any other matter.

12.5 Third-party Processors

Third-party Processors are responsible for ensuring compliance with Data Protection legislation/regulation when processing personal data and also with this Data Protection Policy. Non-compliance may lead to the withdrawal of *HCR* data from that third-party and/or the cancellation of any contract between *HCR* and the third-party processor.

12.6 Joint Data Controllers

Joint Data Controllers are responsible for ensuring compliance with Data Protection legislation/regulation when processing personal data. Non-compliance may lead to the cancellation of any arrangement/agreement/contract that is in place between *HCR* and a Joint Controller.

13. Policy Governance

HCR reserves the right to monitor compliance with this policy and to up-date this policy on the provision of reasonable notice. This Data Protection Policy is not an exhaustive statement of *HCR*'s data protection practices. The manner in which *HCR* process data will evolve over time and policy will be updated from time to time to reflect changing practices. In addition, *HCR* operate a number of other policies and procedures which inter-relate with this policy. In addition, in order to meet its transparency obligations under Data Protection Law, *HCR* may incorporate this Data Protection Policy by reference into notices used at various points of data capture when collecting personal data (e.g., application forms, website forms etc.).

Appendix 1: Glossary of terms

A1.1 Definitions used by the organisation (drawn from the GDPR)

Material scope (Article 2 GDPR) – 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 GDPR) – 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.

A1.2 Article 4 (GDPR) definitions

Child – the GDPR defines a child (for information society services) as anyone under the age of 16 years old, although this may be lowered to 13 by Member State 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.

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.

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.

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.

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.
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.
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.
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.
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.
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.
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.

Appendix 2: Transparency and Data Privacy Notices

In summary, a Data Privacy Notice should include (at minimum) specific information (set out in data protection/ legislation) which informs data subjects of:

- who is collecting the data;
- why it is being collected;
- what legal basis is being relied upon to process the data;
- how it will be processed;
- how long it will be kept for;
- who it will be disclosed to;
- their rights in relation to their personal data.

Specially, the information that must be provided to the data subject as a minimum include:

1. the identify and contact details of *HCR* and, if applicable *HCR*'s representative;
2. the contact details of the Data Protection Officer;
3. the categories of personal data concerned;
4. the purposes of the processing for which the personal data are intended and the legal basis for the processing;
5. notice of whether the data subject is obliged to provide the personal data and the consequences of not providing the personal data;
6. notice of any statutory or contractual requirements underpinning the request to provide personal data;
7. if processing involves automatic decision making or profiling then the notice should provide meaningful information about the automatic decision-making logic and consequences of the processing for the data subject;
8. the period for which the personal data will be stored;
9. 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 the previous processing will be affected;
10. notice of the right to lodge a complaint with *HCR* and the relevant supervisory authority
11. the identities/categories of all natural/legal persons to whom *HCR* could or may transfer personal data;
12. the recipients or categories of recipients of the personal data, where applicable;
13. where applicable, that *HCR* intends to transfer personal data to a recipient in a third country or international organisation and if so, the legal of protection afforded to the data;

14. the transfer terms, i.e., pursuant to a contract including model contractual clauses (SCCs), or other legally approved mechanism;
15. any further information necessary to guarantee "fair and transparent processing" as deemed necessary in consultation with to the DPO.

The disclosures should be made in a manner calculated to draw attention to them.

Wherever possible, Data Protection Notices must be made available at the first point of contact with the data Subject or, if it is not possible on collection, as soon as reasonably practicable thereafter.

Appendix 3: 'Pseudonymisation' and 'Anonymisation'

Pseudonymisation of data means replacing the identifying characteristics of data with a pseudonym, e.g., replacing the name of an *HCR* employee with a number or a value which does not allow the direct identification of the individual. It allows for the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately, and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.

Although pseudonymisation has many uses, it should be distinguished from anonymisation, as it only provides a limited protection for the identity of data subjects in many cases as it still allows identification using indirect means. Where a pseudonym is used, it is often possible to identify the data subject by analysing the underlying or related data. Pseudonymised data must therefore continue to be managed as personal data.

Anonymisation is the process of turning data into a form which does not identify individuals and where identification is not likely to take place. Anonymisation means irreversibly preventing the identification of the individual to whom it related. Data that has been anonymised therefore ceases to be personal data.

Appendix 4: 'Adequacy Decisions'

An up to date list of the countries which have an 'adequacy decision' can be found on the European Commission's Data Protection Website.

As of May 2022, the Commission has made an 'adequacy decision' about the following countries and territories:

Andorra, Argentina, Canada (commercial organisations), Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Republic of Korea, Switzerland , the United Kingdom under the GDPR and the LED, and Uruguay as providing adequate protection.