CDC
Investment works

Data Protection Policy

June 2020

Contents

1. Introduction and Scope

1.1 Purpose

This policy sets out the basic data protection principles and rules governing the collection, handling and use of personal data within CDC. "**Personal data**" may relate to employees, contractors, prospective counterparties, investee companies, third party investment partners, and other individuals (each a "**data subject**") and could include a name, telephone number, email address, but also other identifiers such as IP address, geo-location, financial data, identity numbers, recordings, images, or any other information that relates to an individual in any way. Generally, if you are in doubt if any particular item of information constitutes personal data, it is likely to be personal data.

There are also "special categories" of more sensitive personal data which require a higher level of protection, such as information about an individual's race or ethnicity, religious beliefs, sexual orientation, trade union membership and political opinions, information about health, including any medical condition, health and sickness records, genetic information, biometric data e.g. finger print recognition, information about a person's sex life or sexual orientation and information about criminal convictions and offences. If you are dealing with personal data of this nature (or are likely to) or if you are in doubt, you should seek assistance from our Data Protection Team ("DPO Team").

Personal data may be collected from multiple sources: directly from the individuals (for example, via our websites, or face-to-face), via intermediaries (for example through fund managers, due diligence providers) or through social media and other public sources.

Privacy and personal data are protected by UK and European legislation, as well as legislation in other countries where we operate ("**data protection laws**"). Data protection laws do not prohibit the use of personal data but rather are designed to ensure that personal data is used lawfully in a transparent, proportionate, secure and fair manner for everyone involved. Failure to comply with data protection laws may lead to serious liabilities and consequences for CDC, including the introduction of processing restrictions, fines, claims for damage, serious reputational damage to CDC and loss of business.

CDC is strongly committed to respecting the privacy of its employees, investees, stakeholders and other individuals it deals with in its day-to-day business activities.

1.2 Scope of the Policy

This policy is applicable to all CDC employees, CDC Board and committee members, contractors and third parties who are involved in the processing of personal data. Personal data arises in all aspects of CDC operations including but not limited to, human resources, communications (mailing lists, online information, social media), client relationship management, investment operations, compliance, travel, and information technology.

How does this affect you? This policy goes into some detail but, essentially, we would like you to understand that:

- CDC has to comply with the data protection principles set out in Appendix 2 and this will not be possible without your help and understanding of those principles.
- If your data is processed, you should have access to a data privacy notice, such as the privacy notice for employees and contractors or our website privacy notice. The notice should explain how your data is being processed and what are your rights.
- If you work on a project for CDC you should follow our internal processes to ensure that we stay compliant, such as CDC's personal data processing framework in Appendix 3 or our Privacy by Design and Default and DPIA Procedure.
- Keeping data confidential and secure is half the battle – speak to IT if you are unsure how to achieve that.

- We need to keep an eye on our subsidiaries, suppliers and other third parties to make sure they adhere to data protection principles. Their activities must always be underpinned by a contract as further explained in section 5 below.

- Report any issues or data breaches to the DPO as further explained in section 6 below. Also, if you are unclear about what is expected of you please speak to our data protection team, who are available for guidance.

- We cannot make important decisions (e.g. recruitment) based solely on automated processing (including profiling).

Please refer to the definitions set out in Appendix 1 for a description of commonly used terms.

The following policies, procedures and documents complement this policy and give practical guidance in relation to personal data processing activities:

- Personal Data Breach Procedure
- Personal Data Breach Incident Report Form
- Data Subject Rights Procedure
- Privacy by Design and Default and DPIA procedure
- Consent Management Procedure
- Guidelines on Legitimate Interests
- Information and Cyber Security policy
- Record Retention policy
- CCTV Policy and standard

The Data Protection Officer (DPO) is the sponsor of this policy. For queries, please contact the DPO by email to dataprotection@cdcgroup.com.

2. Roles and responsibilities / Governance

All employees are required to understand the requirements of this policy. Failure to comply with these Policies could result in the Information Commissioner's Office ("ICO") taking action against CDC, and may result in CDC taking disciplinary action in accordance with the Staff Handbook up to and including dismissal.

CDC's senior management and all those in managerial or supervisory roles are responsible for encouraging good personal data management practices throughout CDC.

2.1 CDC Employees and Contractors

All CDC employees and contractors with access to CDC's information systems (together referred to as "Users") must be aware of and comply with the basic data protection principles and the procedures set out in this policy, such as CDC's personal data processing framework in Appendix 3.

Does your work involve the processing of personal data or are you working on a new project? If so, please speak with the DPO or the relevant Personal Data Process Owner ("PDPO") (see section 2.2 below).

All users must complete the required data protection and information security training provided from time to time to keep their knowledge up to date.

2.2 Personal Data Process Owners (PDPO)

The person(s) specifically in charge of the project, operation or process, are referred to in this policy as the "Personal Data Process Owners" or "PDPOs". You may be a PDPO if you are starting a new project in your department.

The PDPOs are responsible for:

- Contacting the DPO about new projects or any matters during the project;
- promptly liaising with the DPO if any individual enquiries about his or her data;

2.3 Data Protection Officer (DPO)

CDC has appointed a DPO to oversee the policies, procedures and controls CDC has established to achieve data protection compliance, to provide guidance, and to act as a point of contact for employees. The name and contact details of the DPO are available on Sydney.

The DPO is responsible for oversight of compliance with privacy and data protection requirements within CDC, including handling compliance with data protection laws. The DPO advises CDC's Board, Audit and Compliance Committee and Executive Committee (ExCo) and employees and contractors where needed. However, the DPO sits within the second line-of-defence and, as such, is not responsible for delivery of compliance. It is the responsibility of each business area to ensure that it complies with GDPR and other relevant data protection requirements, in line with CDC's three line-of-defence control framework.

Pursuant to article 39 of the GDPR, the DPO has the following key responsibilities:

(a) to inform and advise CDC and its employees who carry out processing of personal data of their obligations under GDPR and other relevant data protection provisions;

(b) to monitor compliance with GDPR and CDC policies relating to protection of personal data, including assignment of responsibilities, awareness-raising and training of staff involved in processing operations and related audits;

(c) to provide advice where requested and sign off with regard to data protection impact assessments ("DPIA") and monitor their performance;

(d) to cooperate with the Information Commissioner's Office ("ICO");

(e) to act as a contact point for the ICO on issues relating to processing and to consult with the ICO, where appropriate, with regard to any other matter;

(f) to act as a point of contact for employees and individuals whose data is processed;
(g) to report to CDC's Board and governance committees on matters relating to GDPR compliance.

The DPO shall have due regard to the risks associated with processing operations, taking into account the nature, scope, context and purposes of processing.

The DPO is the owner of this policy and is responsible for maintaining it. The DPO will submit an updated version of the policy to the Audit and Compliance Committee every year for review and approval.

2.4 Audit and Compliance Committee

The Audit and Compliance Committee monitors and reviews the effectiveness of the internal control framework surrounding the data protection compliance programme, policies and procedures put in place to mitigate any related risks.

The DPO will report any significant issues to the Committee.
Internal Audit will periodically review compliance with this policy in accordance with the annual Internal Audit Plan.

2.5 Other governance tools

In order to document compliance with the data protection principles and the GDPR, CDC will deploy the following resources:

- The DPO will advise staff and provide guidance to the business;

- CDC will keep its policies and procedures up-to-date and monitor compliance;
- CDC will provide training to develop a "privacy by design" culture within CDC;
- A record of processing activities will be kept;
- DPIAs will be carried out where appropriate;
- External advice will be sought where appropriate; and
- Other resources will be considered where required.

3. Notification of Privacy Notice to Data Subjects

CDC must ensure that, prior to processing any personal data, the individuals involved are informed, by reference to a **Privacy Notice** (either the privacy notice for employees and contractors or the website privacy notice)**,** of the fact that CDC will be processing their personal data. The privacy notice should, at a minimum, explain the following:

- CDC's name and address (as "controller", meaning the legal entity that is responsible for the processing);
- the specific purposes for which the personal data will be processed;
- the (categories of) other parties with whom the personal data will be shared;
- the existence of the individuals' right of access to and rectification of the personal data (see below); and
- any other information necessary to ensure that the processing is fair.

Please note that failing to provide the privacy notice is likely to delay the project or processing activity. Where CDC does not collect the data directly from the relevant individual or are not in direct contact with them, the PDPO should assess (with guidance from the DPO) whether to contact them proactively or instead rely on information available on demand or published on CDC's website (e.g., where proactively contacting the individual would require disproportionate efforts).

4. Requests from Data Subjects

Users and those in supporting functions must cooperate with the PDPO (with the support the DPO) in complying with all related internal procedures relating to requests from Data Subjects in accordance with the **Data Subject Rights Procedure**.

Individuals may contact CDC to exercise the following rights:

- a right to **receive transparent information** (CDC must inform and communicate with data subjects in a concise, transparent and easily accessible format, using clear and plain language);
- a right of **access to their personal data** (including the purpose of the processing, the categories of personal data concerned, the recipients to whom the personal data have been or will be disclosed, the period for which it is envisaged that the personal data will be stored, the existence of their various rights under data protection law);
- a right to **rectify any information which is outdated or inaccurate**;
- a right to **file a complaint** with the ICO;
- a right to **object to the processing of their personal data in certain circumstances** (e.g., withdrawing consent for direct marketing purposes; or where the processing is based on a legitimate interest, CDC must stop processing personal data, unless it can demonstrate compelling legitimate grounds, such as processing which overrides the interests, rights and freedoms of the data subject, or for the defence of legal claims);
- a right to **restriction of processing** (e.g. where a data subject contests the accuracy of the data held, processing must be suspended for a period to enable CDC to verify the accuracy of that personal data; or where the data subject has objected to the processing); when the processing is restricted, the personal data may only be processed with the data subject's consent and CDC must inform the data subject before the restriction on processing can be lifted;
- a right to **erasure of their personal data**, also known as the "right to be forgotten" (e.g. the data is no longer necessary for the purposes for which they were collected or processed; where the data subject's consent was a pre-condition for the processing and they withdraw their consent; data subject objects to the processing and there are no overriding legitimate or lawful grounds for the processing; the personal data has been unlawfully processed; and the personal data must be erased for compliance with a legal obligation to which CDC is subject); where CDC has made the personal data public and is obliged to erase the personal data, CDC must do what is reasonable or

feasible, taking into account available technology and the cost of implementation, to inform any other related parties which are processing the personal data for their own purposes, that the data subject has requested the erasure;

- a right to **data portability** (only when the processing activity is based on consent or on a contract with the individual), i.e. the right to receive their data or to have the data transmitted to a third party (e.g., an insurance company, a pension company, etc.); the PDPO can continue to process the personal data if the lawful basis for processing is still present; data portability does not automatically trigger the erasure of the personal data from CDC's systems or files and does not affect the retention period applying to the personal data;
- a right to **refuse automated individual decision-making, including profiling** (e.g. a recruitment aptitude test which uses pre-programmed algorithms and criteria impacting on their suitability to be considered for a role at CDC). A data subject has the right not to be subjected to decisions which are based solely on the automated processing of their personal data and so has the right to obtain human intervention on the part of CDC, to express their point of view, and to be able to contest the decision. Further information is set out in Appendix 4.

If you receive such a request from a data subject by telephone, email, letter or by any other means you must contact the DPO and follow the **Data Subject Rights Procedure. Under no circumstances must anyone amend, erase or destroy personal data** to avoid disclosure. It is a criminal offence and may lead to disciplinary action.

5. Third parties

CDC uses third parties (vendors, contractors, suppliers) that have access to personal data. We share the data with other CDC group companies, and we may share personal data with other third parties (e.g. business partners, insurers, financial institutions) for their own business purposes. In this context, the data may be transferred to third parties and CDC group companies established outside the EEA or the UK.

We must comply with certain rules when we involve third parties in the processing of personal data.

5.1 Working together with third parties

CDC may use third party suppliers or contractors to help with data processing activities or CDC may help them in their own activities. When we do so, we must carry out certain due diligence and enter into a **Data Processing Agreement** or include appropriate provisions for data processing in the agreement with that third party.

When we involve third parties in our personal data processing activities, CDC will always remain ultimately responsible towards the individuals and the data protection authorities for anything that happens to personal data. It is extremely important that we carefully select and monitor the external organisations that process personal data on behalf of CDC in accordance with the **Third-Party Security Policy** included in the **Information and Cyber Security policy.**

5.2 Transferring to / Receiving data from third parties

CDC may transfer personal data to third parties for their own business purposes, independent from CDC's purposes, or we may receive personal data from third parties. We should only do so if we have a lawful basis for doing this (for example, consent of the individual, a legal obligation or another appropriate basis). In each case, we will have to enter into a **Data Sharing Agreement** or include appropriate provisions for data sharing in the agreement with that third party.

5.3 Transferring personal data to countries outside the EEA or the UK

Special attention is required if CDC transfers personal data to countries outside the EEA or the UK. A "transfer" has a broad meaning and it will include, for example, remote access by someone outside the EEA or the UK. It is not relevant whether such person actively uses our data or provides more passive services such as back-up.

Export of personal data from the EEA or the UK to a country outside the EEA or the UK is permitted only where the recipient is in a "trusted" country or where certain other measures are put in place as set

out in **Appendix 5**. Please contact the DPO before proceeding to transfer personal data to any third party established in a country outside the EEA or the UK.

6. Information security / dealing with data related incidents

Each of us has a duty of care to keep personal data secure from unwanted, unauthorised and unlawful use, modification or access, to follow the rules established by the relevant PDPO, and the **Information and Cyber Security policy**.

Upon discovery of a personal data breach or a suspected personal data breach all CDC employees (regardless of which office they work in), contractors and authorised third parties must report it as soon as possible in accordance with the **Personal Data Breach Procedure**, which requires submission of a **Data Breach Incident Report Form** to the DPO and the Chief Legal Officer. Personal data breaches (and security breaches that may cause a personal data breach) may include, or occur as a result of:

- Loss or theft of data or equipment on which data is stored;
- Inappropriate access controls allowing unauthorised use;
- Equipment failure;
- Human error;
- Unforeseen circumstances such as a fire or flood;
- Hacking; or
- Blagging offences where information is obtained by deception.

It is vital that the personal data breach is reported **as soon as possible**. If a personal data breach has to be reported to the ICO it must be notified within 72 hours of the data controller becoming aware of the breach. Failure to notify a personal data breach can result in significant fines (including if the breach is notified late, e.g. not within the 72-hour period for data controllers).

7. Contact with Authorities

All contacts with any government authority or agency, such as the Information Commissioner's Office (ICO), or Her Majesty's Revenue and Customs (HMRC), whether or not this is a CDC initiated contact, with respect to any matter related to CDC's personal data processing activities must go through the DPO.

If you are contacted by any government authority or agency, with a request to access personal data that is processed by CDC, with questions regarding CDC's processing activities or during an investigation, you must immediately contact the DPO.

Appendix 1 - Definitions

Term	Definition
Controller	The legal CDC entity (CDC / CDC group) which alone or jointly with others determines the purposes and means of the processing of the personal data.
Data Protection Impact Assessment (DPIA)	Where a processing which is envisaged in the framework of a project, in particular one using new technologies, and taking into account the nature, scope, context and purposes of that processing, is likely to result in a high risk for the rights and freedoms of data subjects, the controller must, before starting the processing, carry out an assessment of the impact of that envisaged processing on the protection of these data subjects' personal data.
Data subject	A natural person whose personal data are processed.
Data Protection Officer (DPO)	The person(s) appointed by CDC management to take the lead in supporting and organising CDC's data privacy compliance structure and activities. Their name(s) can be found on CDC's intranet (SharePoint).
Lawful basis	The processing of Personal data is lawful only if it has one of the following justifications: (a) the data subject has given consent to the processing of their Personal data for one or more specific purposes; (b) the 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; (c) processing is necessary for compliance with a legal obligation to which the controller is subject; (d) processing is necessary for the purposes of the legitimate interests pursued by the controller 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; (e) processing is necessary in order to protect the vital interests of the data subject or of another natural person; (f) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.
Personal Data Process Owner (PDPO)	The business or corporate function / division / department within CDC, which is responsible for the project and the related processing of the personal data (as part of the project), and which determines the purposes and the means of the processing activities.
Personal data	Any data relating to an identified or identifiable natural person (data subject). An identifiable person is one who can be identified, directly or indirectly, by reference. Examples: name, telephone, home address, photo, video, IP address, interests / preferences, behavioural patterns / profiling, subscription data, outcome of surveys, financial info, identity document.
Processing (of Personal data)	Any operation which is performed on personal data, whether or not by automated means, such as (non-exhaustive) collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, transfer, (remote) access, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.
Processor	Any entity processing personal data on behalf of the controller (usually based on a data processing or other service agreement).
Project	Any project or activity undertaken by a business or corporate function, such as providing a new service, launching an app, putting in place a new technology or a new process (business, hr…), setting up a website, a portal, a new IT support system or application, etc., which involves the processing of personal data.
Third Party	Any third party providing products to or performing services for CDC. may also include a third parties affiliated companies, subcontractors, consultants, service providers, suppliers…

Appendix 2 - Key principles of data protection

When processing personal data, we should always comply with the following key principles:

1. **Lawfulness, fairness and transparency:** CDC's processing activities must be always based on one of the lawful bases foreseen in data protection laws (see below). Each individual must be informed about how their data is being processed by way of a privacy notice written in clear and plan language. Fairness is an overarching principle which generally means that our processing of personal data should not be unexpected, and we must mitigate any adverse effects. **Purpose limitation:** Subject to limited exceptions, we only process personal data for purposes that are specified, informed to the person and legitimate (i.e. with a lawful basis and within the legitimate expectations of the individual); we do not further process the personal data for another purpose.

   Example: *if we process data that we collected for the purposes of conducting a survey, we should not use such data for pro-active marketing activities related to our events or other services unless the individual specifically consented to such activities.*

2. **Data minimisation:** We limit the collection and use of personal data to what is directly relevant and necessary for the purposes for which we need to process them.
3. **Accuracy:** We must keep the personal data accurate and up to date; we should not keep data that is inaccurate, and we should implement processes to maintain the accuracy/quality of the data.

4. **Storage limitation:** We must not keep the personal data for longer than is necessary based on the retention period defined in the **Record Retention policy**; once the personal data is no longer necessary for the purposes for which it was collected, we must erase or anonymise it.

   Example: *If we collect personal data for a research purposes, once the research has been performed and the results are obtained we should erase the personal data and only keep the results (generally: statistical information) on a no-name basis.*

5. **Data security:** We must implement appropriate technical and organisational measures to ensure a proper level of security of the personal data; the measures must provide for the prevention of any unauthorised disclosure of the data or any unauthorised access to it, accidental or unlawful deletion, loss or alteration of the data or any other unlawful or unauthorised form of action regarding the data.

6. **Accountability:** We must be able to demonstrate compliance by putting in place policies, procedures and training and keeping a record of processing.

Lawful Basis: Below are applicable lawful bases for common CDC processes

Lawful basis	Examples
(i) CDC has obtained the **unambiguous consent** of the individual (for example, through a specific consent form). The consent must be specific to the individual processing(s) and purpose(s), not a general one. Records of consent must be kept for proof. *Please refer to the **Consent Management Procedure** when selecting and using consent as a lawful basis for processing.*	✚ Conducting a survey whereby the individual has signed a paper consent form or approved an online consent form ✚ (In cases where we are not relying on legitimate interest – see below) Sending event/service information based on consent collected when visiting an event or website

(ii) The processing is necessary for the **performance of a contract between CDC and the individual** (or in order to take certain steps at the request of the individual prior to entering into a contract). It must be a contract to which the individual is (or will be) a party. The processing of the personal data must be a necessity for the performance of the contract; CDC must be able to demonstrate that CDC would not be able to perform its contractual engagements without processing the personal data.	✚ Using a bank account number for the payment of an employee's salary ✚ Using contact data to send investment related information to an investee or fund manager ✚ Reviewing candidate personal information contained within CVs as part of a recruitment process
(iii) The processing is necessary for the purpose of the **legitimate interests pursued by CDC**, except where such interests are outweighed by the privacy rights of the individuals. CDC must: ✚ clearly define what our business interest is and why it is legitimate; ✚ identify the rights and interests of the individual, which might be conflicting with or jeopardised by CDC's business interest; ✚ perform a balancing test whereby CDC must justify that its legitimate interest is not outweighed by the rights or interests of the individual. CDC must document this balancing test. *Please contact the DPO when considering processing personal data on such basis and refer to the **Guidelines on Legitimate Interest**.*	✚ Monitoring employees for safety or management purposes (such as performance evaluations) if appropriate safeguards have been implemented ✚ Most HR systems that do not fall under (iv) below ✚ Monitoring users for physical security or IT and network security if appropriate safeguards have been implemented ✚ Storing and using contact information of individuals working at other businesses, insofar as such use of their data is limited to the scope of CDC's and their business ✚ Sending newsletters or other bulk mailings to update stakeholders about our business.
(iv) The processing is necessary to **comply with a legal obligation of CDC**.	✚ Using an individual's personal information to fill in a legally mandatory employment declaration to relevant authorities ✚ Performing screening of employees and investees under financial and anti-money-laundering rules ✚ Reporting certain suspicious financial transactions to the competent authorities under anti-money-laundering rules
(v) The processing is necessary to **protect the vital interests** of the individual. *Please contact the DPO when you consider processing personal data on such basis.*	✚ emergency medical care, when CDS needs to process personal data for medical purposes, but the individual is incapable of giving consent to the processing
(vi) The processing is necessary to perform a task carried out **in the public interest or in the exercise of official authority** vested in the controller or a third party to whom data are disclosed. *Please contact the DPO when you consider processing personal data on such basis.*	(This lawful basis is unlikely to apply to CDC)

Appendix 3 - CDC's personal data processing framework

When designing / reviewing a processing activity:

- Inform and consult with the DPO before design, implementation and review of your processing activity.
- Complete a **Data Process Map Template** describing in detail your processing activity – including the data sources, the data flows, the full list of data categories, the purposes of the processing, the involvement of third parties and their roles, etc. This information will feed into CDC's data protection records, which it is obliged to maintain. Further information on the **Data Process Map Template** and how to use it can be obtained from the DPO.
- Important points to keep in mind when working on the "Data Process Map Template":
  - Check what your lawful basis for processing is and document it.
    The ICO has published a tool to assess which lawful basis is most appropriate for a given processing activity (https://ico.org.uk/for-organisations/resources-and-support/getting-ready-for-the-GDPR-resources/lawful-basis-interactive-guidance-tool/lawful-basis-assessment-report/). The DPO can also provide support to select the correct lawful basis for processing personal data.
  - Make sure that you only process personal data that is directly relevant and necessary for purposes of your processing.
  - Seek advice from DPO if you intend to process sensitive or criminal conviction data.
- If the processing is based on the consent of the individuals, follow the guidance set out in the **Consent Management Procedure**.
- Consult with the DPO and Business Services to set clear rules and processes to ensure data security.
- Agree a data retention period and inform Business Services to implement processes to ensure personal data can be updated, cleaned-up, deleted or anonymised when required.
- Involve a member of CDC's Legal team to ensure that CDC enters into appropriate data processing contracts or agreements with third parties (business partners, vendors, suppliers, and in some cases, other CDC group companies and subsidiaries).
- With guidance from the DPO, consider whether a new privacy notice is required for the process to relay information transparently to the individuals concerned. If so, prepare the appropriate privacy notice– and make the notice available to them in consultation with the Communications team.
- In some circumstances where individuals' privacy is potentially at a higher risk, PDPOs must also perform a Data Protection Impact Assessment (DPIA), with guidance from the DPO. For more information on this, refer to the **Data Protection Impact Assessment Procedure.**

Before collecting personal data:

- Make sure that you have the proper lawful basis in place before you proceed with the collection of personal data. This means relying on a lawful basis for processing (e.g. a contract between CDC and the individual, a legitimate interest that CDC can demonstrate), or otherwise having obtained the individuals' consent and, unless the DPO confirms this is not required, notify the individual of the relevant privacy notice.

When processing personal data:

- Keep the data secure, only share it on a strict need-to-know basis and within the limits of the purposes of the processing.
- Keep the data accurate and up-to-date; delete or anonymise it when no longer needed in accordance with the **Record Retention policy**.

Ongoing compliance:

- Keep data processing activities under review: if the data processing activities change (which may be because of changes made by a third party supplier) you may need to provide a new **Privacy Notice** which sets out the new purpose, the new lawful basis for processing or other relevant change.
- Ensure all new staff receiving proper training and all members of staff receive refresher training.
- Ensure all documentation and records are kept up to date.

Appendix 4 - Transfer of personal data to countries outside the EEA (applicable to intra-group transfers and transfers to third parties)

1. *Transfer to a country that provides "an adequate level of data protection" (the "trusted" countries)*

The European Commission has so far recognised the following non-EEA countries as ensuring "an adequate level of data protection", known as the "trusted" countries. So, personal data can be transferred legally to these countries.

- Andorra
- Argentina
- Canada (but only where the data transferred is subject to the Canadian Personal Information Protection and Electronic Documents Act)
- Faroe Islands
- Guernsey
- Isle of Man
- Israel
- Japan (private sector entities only)
- Jersey
- New Zealand
- Switzerland
- Uruguay
- USA (limited to entities certified under the Privacy Shield framework – see https://www.privacyshield.gov/list)

Note: Adequacy talks are ongoing with South Korea.

2. *Conditions for transfer outside the EEA to a country that does not provide "an adequate level of data protection"*

CDC may transfer personal data to third parties (including CDC group companies) established in countries outside the EEA, but only in certain specific circumstances.

One of these circumstances is where the individual has given their explicit consent to the transfer. The most relevant circumstance that CDC would be allowed to transfer data to organisations in such countries is where adequate safeguards have been put in place to protect the transferred personal data, such as appropriate contractual clauses and GDPR compliance audits of the non-EEA recipient:

- The European Commission has approved certain "standard contractual clauses" which can be used by CDC in its contracts with a non-EEA recipient to ensure that the individual's privacy is adequately protected. These standard contractual clauses are available from: http://ec.europa.eu/justice/data-protection/document/international-transfers/transfer/index_en.htm.
- Approved codes of conduct can be used to transfer personal data internationally within the same corporate group, providing the requirements of Article 40 of the GDPR are followed, and where there is a binding and enforceable commitment of the controller or processor in the third country to apply appropriate safeguards.
- The European Commission can approve "binding corporate rules" which are similar to an approved code of conduct, in that they allow multinational companies to transfer personal data internationally within the same corporate group, ensuring that the individual's privacy is adequately protected. The process for binding corporate rules can be found at: https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/binding-corporate-rules_en. further information can be found at: https://ico.org.uk/for-organisations/guide-to-data-protection/binding-corporate-rules/.
  Each time the processing activity you are involved in includes data transfers to countries outside the EEA, make sure that the relevant PDPO is involved in a timely manner **before** data processing commences. If you are the PDPO, you should contact the DPO in a timely manner and they will then support you in implementing an appropriate mechanism for your data processing activities.

Investment works

CDC Group plc
123 Victoria Street
London SW1E 6DE
United Kingdom
+44 (0)20 7963 4700

cdcgroup.com

linkedin.com/company/cdc-group-plc

@CDCgroup