GDPR Data Protection Policy

Date June 2018

Version 0.1

Contents

1. Documentation and approvals

1.1. Revision history

This document is subject to revision control. The master electronic copy can be found at SharePoint

Version	Revision date	Summary of changes	Author
14	19/07/2018	GDPR approved	Shuja and Simon

1.2. Approvals

The document requires the following approvals:

Name	Signature	Position	Date approved	Version
Ops group (SMT)		Senior Management Team	03 June	14

1.3. Distribution

This document has been distributed to:

Distribution list	Date of issue	No. of copies
All ClientEarth staff [in London, Warsaw, New York and Brussels]		

2. Introduction

ClientEarth is committed to conducting its business in accordance with all applicable Data Protection laws and regulations and in line with the highest standards of ethical conduct.

This policy details expected behaviours of ClientEarth's Employees and Third Parties in relation to the collection, use, retention, transfer, disclosure and destruction of any Personal Data belonging to a ClientEarth Customer and Staff (i.e. the Data Subject) and irrespective of the media used to store the information.

Personal Data is any information (including opinions and intentions) which relates to an identified or Identifiable Natural Person. Personal Data is subject to certain legal safeguards and other regulations, which impose restrictions on how organisations may process Personal Data.

An organisation that handles personal data and makes decisions about its use is known as a Data Controller. ClientEarth, as a Data Controller, is responsible for ensuring compliance with the Data Protection requirements outlined in this policy.

Non-compliance may expose ClientEarth to complaints, regulatory action, fines and/or reputational damage.

ClientEarth's leadership is fully committed to ensuring continued and effective implementation of this policy and expects all ClientEarth Employees and Third Parties to share in this commitment.

Any breach of this policy will be taken seriously and may result in disciplinary action or business sanction.

3. Scope

3.1. This policy applies to all ClientEarth Entities where a Data Subject's personal data is processed in the context of the business and/or charitable activities of the ClientEarth Entity.

3.2. This policy applies to all processing of personal data in electronic form (including electronic mail and documents created with word processing software) or where it is held in manual files that are structured in a way that allows ready access to information about individuals.

3.3. This policy has been designed to establish a baseline standard for the processing and protection of personal data by all ClientEarth Employees. Where national law imposes a requirement that is stricter than that imposed by this policy, the requirements in national law must be followed. Furthermore, where national law imposes a requirement that is not addressed in this policy, the relevant national law must be adhered to.

3.4. Each department within ClientEarth should have a Privacy Champion, who is responsible for overseeing their department's compliance with this Data Protection Policy and, as applicable, developing Related Policies and Privacy Guidelines.

3.5. Please contact your department's Privacy Champion with any questions about the operation of this Data Protection Policy or the General Data Protection Regulation or if you have any concerns that this Data Protection Policy is not being or has not been followed. In particular, you should contact your department's Privacy Champion in the following circumstances:

3.5.1. if you are unsure of the lawful basis which you are relying on to process Personal Data (including the legitimate interests used by ClientEarth);

3.5.2. if you need to rely on Consent and/or need to capture Explicit Consent;

3.5.3. if you need to draft Privacy Notices or Fair Processing Notices;

3.5.4. if you are unsure about the retention period for the Personal Data being Processed;

3.5.5. if you are unsure about what security or other measures you need to implement to protect Personal Data;

3.5.6. if there has been a Personal Data Breach;

3.5.7. if you are unsure on what basis to transfer Personal Data outside the EEA;

3.5.8. if you need any assistance dealing with any rights invoked by a Data Subject;

3.5.9. whenever you are engaging in a significant new, or change in, Processing activity which is likely to require a DPIA or plan to use Personal Data for purposes others than what it was collected for;

3.5.10. if you plan to undertake any activities involving Automated Processing including profiling or Automated Decision-Making;

3.5.11. if you need help complying with applicable law when carrying out direct marketing activities; or

3.5.12. if you need help with any contracts or other areas in relation to sharing Personal Data with third parties (including our vendors).

4. Definitions

TERM	DEFINITION
Anonymisation	Data amended in such a way that no individuals can be identified from the data (whether directly or indirectly) by any means or by any person.
Binding Corporate Rules	The Personal Data protection policies used for the transfer of Personal Data to one or more Third Countries within a group of undertakings, or group of enterprises engaged in a joint economic activity.
Consent	Any freely given, specific, informed and unambiguous indication of the Data Subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the Processing of Personal Data relating to him or her.
Customer	Any past, current or prospective ClientEarth customer.
Data Controller	A 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.
Data Processors	A natural or legal person, Public Authority, Agency or other body which Processes Personal Data on behalf of a Data Controller.
Data Protection	The process of safeguarding Personal Data from unauthorised or unlawful disclosure, access, alteration, Processing, transfer or destruction.
Data Subject	Anyone 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 one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
EEA	The 28 countries in the EU, and Iceland, Liechtenstein and Norway.
Employee	An individual who works part-time or full-time for ClientEarth under a contract of employment, whether oral or written, express or implied, and has recognised rights and duties - includes temporary employees and independent contractors.
Encryption	The process of encoding a message or information in such a way that only authorised parties can access it.
Information Commissioner's Office (ICO)	An independent Public Authority in the UK responsible for monitoring the application of the relevant Data Protection regulation set forth in national law.
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.
Privacy Champion	An individual appointed by an organisation, such as ClientEarth, on a voluntary basis and tasked with the enforcement of the values of the GDPR and the organisation's Data Protection Policy, in addition to being a point of contact for any internal and external queries relating to data protection.
Process, Processed, Processing	Any operation or set of operations performed on Personal Data or on sets of Personal Data, whether or not by automated means. Operations performed

	may include collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
Profiling	Any form of automated processing of Personal Data, where Personal Data is used to evaluate specific or general characteristics relating to a data subject. In particular to analyse or predict certain aspects concerning that natural person's performance at work, economic situations, health, personal preferences, interests, reliability, behaviour, location or movement.
Pseudonymisation	Data amended in such a way that no individuals can be identified from the data (whether directly or indirectly) without a "key" that allows the data to be re-identified.
Special Categories of Data	Personal Data pertaining to or revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, data concerning health or sex life and sexual orientation, genetic data or biometric data.
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;
GDPR	General Data Protection Regulation
DPO	Data Protection Officer
DPIA	Data Protection Impact Assessment
Privacy Notices	ClientEarth Privacy notice on CE website

5. Policy

5.1. GOVERNANCE

5.1.1. POLICY DISSEMINATION AND ENFORCEMENT

The management team of ClientEarth must ensure that all ClientEarth Employees responsible for the Processing of Personal Data are aware of and comply with the contents of this policy. In addition, ClientEarth will make sure all Third Parties engaged to Process Personal Data on their behalf (i.e. their Data Processors) are aware of and comply with the contents of this policy. Assurance of such compliance must be obtained from all Third Parties, whether companies or individuals, prior to granting them access to Personal Data controlled by ClientEarth.

5.1.2. DATA PROTECTION BY DESIGN

To ensure that all Data Protection requirements are identified and addressed when designing new systems or processes and/or when reviewing or expanding existing systems or processes, each of them must go through an approval process before continuing.

ClientEarth must ensure that a Data Protection Impact Assessment (DPIA) is conducted, for all new and/or revised systems or processes for which it has responsibility. ClientEarth should consult with a Data Protection subject matter expert during the course of completing the DPIA. The subsequent findings of the DPIA must then be submitted to the senior risk office for ClientEarth for review and approval. Where applicable, the Information Technology (IT) department, as part of its IT system and application design review process, will cooperate with the Data Protection subject matter expert to assess the impact of any new technology uses on the security of Personal Data.

5.2. PRINCIPLES

5.2.1. DATA PROTECTION

ClientEarth has adopted the following principles to govern its collection, use, retention, transfer, disclosure and destruction of Personal Data.

PRINCIPLE	DEFINITION
Principle 1: Lawfulness, Fairness and Transparency	Personal Data shall be processed lawfully, fairly and in a transparent manner in relation to the Data Subject. This means, ClientEarth must tell the Data Subject what Processing will occur (transparency), the Processing must match the description given to the Data Subject (fairness), and it must be for one of the purposes specified in the applicable Data Protection regulation (lawfulness).
Principle 2: Purpose Limitation	Personal Data shall be collected for specified, explicit and legitimate purposes and not further Processed in a manner that is incompatible with those purposes. This means ClientEarth must specify exactly what the Personal Data collected will be used for and limit the Processing of that Personal Data to only what is necessary to meet the specified purpose.

Principle 3: Data Minimisation	Personal Data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are Processed. This means ClientEarth must not store any Personal Data beyond what is strictly required.
Principle 4: Accuracy	Personal Data shall be accurate and kept up to date. This means ClientEarth must have in place processes for identifying and addressing out-of-date, incorrect and redundant Personal Data.
Principle 5: Storage Limitation	Personal Data shall be kept in a form which permits identification of Data Subjects for no longer than is necessary for the purposes for which the Personal Data is Processed. This means ClientEarth must, wherever possible, store Personal Data in a way that limits or prevents identification of the Data Subject.
Principle 6: Integrity & Confidentiality	Personal Data shall be 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. ClientEarth must use appropriate technical and organisational measures to ensure the integrity and confidentiality of Personal Data are maintained at all times.

5.2.2. ACCOUNTABILITY

The Data Controller shall be responsible for, and be able to demonstrate compliance. This means ClientEarth must demonstrate that the six Data Protection Principles (outlined above) are met for all Personal Data for which it is responsible.

5.3. DATA COLLECTION

Personal Data should be collected only from the Data Subject unless one of the following applies:

- The nature of the business purpose necessitates collection of the Personal Data from other persons or bodies.
- The collection must be carried out under emergency circumstances in order to protect the vital interests of the Data Subject or to prevent serious loss or injury to another person.
- If Personal Data is collected from someone other than the Data Subject, the Data Subject must be informed of the collection unless one of the following apply:
  - The Data Subject has received the required information by other means.
  - The information must remain confidential due to a professional secrecy obligation.
  - A national law expressly provides for the collection, Processing or transfer of the Personal Data.

Where it has been determined that notification of such information to a Data Subject is required, notification should occur promptly, but in no case later than:

- One calendar month from the first collection or recording of the Personal Data;
- At the time of first communication, if used for communication with the Data Subject; or
- At the time of disclosure, if disclosed to another recipient.

5.3.1. DATA SUBJECT CONSENT

ClientEarth will obtain Personal Data only by lawful and fair means and, where appropriate, with the knowledge and Consent of the individual concerned.

Where a need exists to request and receive the Consent, via an agreement or positive action, from an individual prior to the collection, use or disclosure of their Personal Data, ClientEarth is committed to seeking such Consent.

ClientEarth shall establish a system for obtaining and documenting Data Subject consent for the collection, processing, and/or transfer of their personal data, for each business operation and department that requires consent (HR, Finance, Communications, Programmes, Admin & IT etc). The system must include provisions for:

- Determining what disclosures should be made in order to obtain valid Consent.
- Ensuring the request for Consent is presented in a manner which is clearly distinguishable from any other matters, is made in an intelligible and easily accessible form, and uses clear and plain language.
- Ensuring the Consent is freely given (i.e. is not based on a contract that is conditional to the processing of Personal Data that is unnecessary for the performance of that contract).
- Documenting the date, method and content of the disclosures made, as well as the validity, scope, and volition of the Consents given.
- Providing a simple method for a Data Subject to withdraw their Consent at any time.

Where a need exists to request and receive the Consent, via an agreement or positive action, from an individual prior to the collection, use or disclosure of their Personal Data, ClientEarth is committed to seeking such Consent.

5.3.2. DATA SUBJECT NOTIFICATION

ClientEarth will when required by applicable law, contract, or where it considers that it is reasonably appropriate to do so, provide Data Subjects with the following information:

- The categories of the Personal Data that is processed;
- The purposes and legal basis for the Processing;
- The duration of the retention of the Personal Data (refer to Data Retention Policy)
- The source from where the Personal Data was collected or received (where applicable);
- Any Third Parties, including those outside the EEA, to whom the Personal Data is or will be disclosed;
- The existence of Data Subject Rights, including to request access to and require restriction, deletion and rectification of the Personal Data;
- The Data Subject's right to lodge a complaint with the ICO.

When the Data Subject is asked to give Consent to the Processing of Personal Data, and when any Personal Data is collected from the Data Subject, all appropriate disclosures will be made, in a manner that draws attention to them, unless one of the following apply:

- The Data Subject already has the information
- A legal exemption applies to the requirements for disclosure and/or Consent.

The disclosures may be given orally, electronically or in writing. If given orally, the person making the disclosures should use a suitable script. The associated receipt or form should be retained, along with a record of the facts, date, content, and method of disclosure.

5.3.3. EXTERNAL PRIVACY NOTES

Each external website provided by ClientEarth will include an online 'Privacy Notice' fulfilling the requirements of applicable law. ClientEarth will also produce a separate Recruitment Privacy Notice to detail how personal data is used during the recruitment process.

5.4. DATA USE

5.4.1. DATA PROCESSING

ClientEarth uses the Personal Data of its staff and partners for the following broad purposes:

- The general running and business administration of ClientEarth.
- When negotiating with suppliers and other business parties.
- To organise events in the charity and advocacy sectors.
- To organise and research particular campaigns.
- To provide newsletters and campaign updates to signatories.
- To research potential donors and beneficiaries in order to approach them.

The use of staff and partner's information should always be considered from their perspective and whether the use will be within their expectations or if they are likely to object. For example, it would clearly be within staff and partner's expectations that their details will be used by ClientEarth to respond to staff and partner's request for information about the products and services on offer. However, it will not be within their reasonable expectations that ClientEarth would then provide their details to Third Parties for marketing purposes.

ClientEarth will Process Personal Data in accordance with all applicable laws and applicable contractual obligations. In particular, ClientEarth will only process personal data in accordance with the legal basis listed in the Records of Processing Activities. In particular, this will always include at least one of the following requirements being met:

- The Data Subject has given Consent to the Processing of their Personal Data for one or more specific purposes.
- 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.
- Processing is necessary for compliance with a legal obligation to which the Data Controller is subject.
- Processing is necessary in order to protect the vital interests of the Data Subject or of another natural person.
- 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 Data Controller.
- Processing is necessary for the purposes of the legitimate interests pursued by the Data Controller or by a Third Party (except where such interests are overridden by the interests or

fundamental rights and freedoms of the Data Subject, in particular where the Data Subject is a child).

There are some circumstances in which Personal Data may be further processed for purposes that go beyond the original purpose for which the Personal Data was collected.

5.4.2. SPECIAL CATEGORIES OF DATA

Special categories or data (also known as sensitive data) include the following:

- Racial or ethnic origin;
- Political opinions;
- Religious or philosophical beliefs;
- Trade union membership;
- Data concerning sex life, sexual orientation or health;
- Genetic data; and
- Biometric data, where processed in a manner that will uniquely identify a person.

ClientEarth will only Process Special Categories of Data where the Data Subject expressly Consents to such Processing or where one of the following conditions apply:

- The Processing relates to Personal Data which has already been made public by the Data Subject.
- The Processing is necessary for the establishment, exercise or defence of legal claims, in particular, relating to discrimination claims in the Employment context.
- The Processing is specifically authorised or required by law, including in the Health and Safety context and for compliance with Equality Monitoring legislation.
- The 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.
- Further conditions, including limitations, based upon national law related to the Processing of genetic data, biometric data or data concerning health.

Where Special Categories of Data are being Processed, ClientEarth will adopt additional protection measures.

5.4.3. DATA QUALITY

ClientEarth will adopt all necessary measures to ensure that the Personal Data it collects and Processes is complete and accurate in the first instance, and is updated to reflect the current situation of the Data Subject.

The measures adopted by ClientEarth to ensure data quality include:

- Correcting Personal Data known to be incorrect, inaccurate, incomplete, ambiguous, misleading or outdated, even if the Data Subject does not request rectification.
- Keeping Personal Data only for the period necessary, to satisfy the permitted uses or applicable statutory retention period.
- The removal of Personal Data if in violation of any of the Data Protection principles or if the Personal Data is no longer required.

- Restriction, rather than deletion of Personal Data, insofar as:
  - A law prohibits erasure.
  - Erasure would impair legitimate interests of the Data Subject.
  - The Data Subject disputes that their Personal Data is correct and it cannot be clearly ascertained whether their information is correct or incorrect.

5.4.4. DIRECT MARKETING

As a general rule, ClientEarth will not send promotional or direct marketing material to members of the public or newsletter subscribers through digital channels such as mobile phones, email and the Internet, without first obtaining their Consent.

The GDPR and Privacy and Electronic Communications Regulations (which govern Direct Marketing Activities within the EU) imports the GDPR standard for consent. That is:

- The consent must be freely given, specific, informed and unambiguous;
- The consent must be expressed by a statement or clear affirmative action. Silence, pre-ticked boxes or inactivity should therefore not constitute consent.
- The consent must be as easy to withdraw as it was to provide consent in the first place.
- The organisation must be able to demonstrate that the individual has consented
- The consent language must be intelligible and use clear and plain language

ClientEarth will not contact recipients via email to establish whether consent is in place, apart from to 'refresh' existing consent.

Where Personal Data Processing is approved for digital marketing purposes, the Data Subject must be informed at the point of first contact that they have the right to object, at any stage, to having their data Processed for such purposes. If the Data Subject puts forward an objection, digital marketing related Processing of their Personal Data must cease immediately, and their details should be kept on a suppression list with a record of the opt-out decision, rather than being completely deleted.

In the context of mailing lists received from partner organisations, ClientEarth will take steps to receive assurances from such partner organisations that such data subjects have given their consent to be placed on such mailing lists. Additionally, ClientEarth will ensure that the context or category of updates, newsletters or campaigns that such individuals have signed up to receive covers both ClientEarth as an organisation and the updates, newsletters or campaigns provided by ClientEarth. ClientEarth will also ensure that it informs such individuals about their right to opt-out from receiving such communications, as outlined above, alongside informing them about how their details were received by ClientEarth.

Additionally, in the context of business-to-business marketing, for example, sending the Access to Justice newsletter to business contacts including lawyers, judges and other partner organisations, ClientEarth, whilst not needing to collect the consent of such individuals, will ensure that they are provided with the adequate notice of their right to object to receiving such materials.

5.5. DATA RETENTION

To ensure fair Processing, Personal Data will not be retained by ClientEarth ClientEarth for longer than necessary in relation to the purposes for which it was originally collected, or for which it was further Processed.

The length of time for which ClientEarth needs to retain Personal Data is set out in the ClientEarth Data Retention Policy and/or in the Records of Processing Activities. This takes into account the legal and contractual requirements, both minimum and maximum, that influence the retention periods set forth in the schedule. All Personal Data should be securely deleted or destroyed as soon as possible where it has been confirmed that there is no longer a need to retain it. For detailed information, please refer to Data Retention Policy.

5.6. DATA PROTECTION

5.6.1. ClientEarth will adopt physical, technical, and organisational measures to ensure the security and protect the confidentiality, integrity and availability of the Personal Data, defined as follows:

- Confidentiality means that only people who have a need to know and are authorised to use the Personal Data can access it.
- Integrity means that Personal Data is accurate and suitable for the purpose for which it is processed.
- Availability means that authorised users are able to access the Personal Data when they need it for authorised purposes

This includes the prevention of loss or damage, unauthorised alteration, access or Processing, and other risks to which it may be exposed by virtue of human action or the physical or natural environment.

5.6.2. A summary of the Personal Data related security measures is provided below:

- Prevent unauthorised persons from gaining access to data processing systems in which Personal Data are processed.
- Prevent persons entitled to use a data processing system from accessing Personal Data beyond their needs and authorisations.
- Ensure that Personal Data in the course of electronic transmission during transport cannot be read, copied, modified or removed without authorisation.
- Ensure that access logs are in place to establish whether, and by whom, the Personal Data was entered into, modified on or removed from a data processing system.
- Ensure that in the case where Processing is carried out by a Data Processor, the data can be processed only in accordance with the instructions of the Data Controller.
- Ensure that Personal Data is protected against undesired destruction or loss.
- Ensure that Personal Data is not kept longer than necessary.
- Regularly evaluate and test the effectiveness of safeguards to ensure security of Processing of Personal Data.

5.7. DATA SUBJECT REQUESTS

5.7.1. ClientEarth will take all steps to facilitate the exercise of Data Subject Requests by employees, interns, volunteers, beneficiaries, newsletter signatories and any other Data Subjects whose personal data is processed. No administration fee will be charged for considering and/or complying with such a request unless the request is deemed to be unnecessary or excessive in nature.

5.7.2. Data Subjects are entitled to, based upon a request made in and upon successful verification of their identity, the following information about their own Personal Data:

- The purposes of the collection, Processing, use and storage of their Personal Data;
- The source(s) of the Personal Data, if it was not obtained from the Data Subject;
- The categories of Personal Data stored for the Data Subject;
- The recipients, or categories of recipients, to whom the Personal Data has been or may be transmitted, along with the location of those recipients;
- The envisaged period of storage for the Personal Data or the rationale for determining the storage period;
- The use of any automated decision-making, including Profiling;
- The retention periods applied to the data; and
- A summary of the security measures in place to protect the data
- Request to erase Personal Data if it is no longer necessary in relation to the purposes for which it was collected or processed or to rectify inaccurate data or to complete incomplete data.

5.7.3. A response to each request will be provided within 30 days of the receipt of the written request from the Data Subject. That period may be extended by two further months where necessary, taking into account the complexity and number of the requests.

5.7.4. Appropriate verification must confirm that the requestor is the Data Subject or their authorised legal representative. Data Subjects shall have the right to require ClientEarth to correct or supplement erroneous, misleading, outdated, or incomplete Personal Data.

5.7.5. Please refer to the Individuals Rights Policy for detailed guidance and procedures for responding to such requests.

5.8. THIRD PARTY DATA

5.8.1. It should be noted that situations may arise where providing the information requested by a Data Subject would disclose Personal Data about another individual. In such cases, information must be redacted or withheld as may be necessary or appropriate to protect that person's rights.

5.8.2. When Personal Data is collected indirectly (for example, from a third party or publicly available source), ClientEarth will provide the Data Subject with all the information required by the GDPR as soon as possible after collecting/receiving the data and, at the latest, within one month.

ClientEarth will also check that the Personal Data was collected by the third party in accordance with the GDPR and on a basis which contemplates proposed Processing of that Personal Data.

5.9. LAW ENFORCEMENT REQUESTS & DISCLOSURES

5.9.1. In certain circumstances, it is permitted that Personal Data be shared without the knowledge or Consent of a Data Subject. This is the case where the disclosure of the Personal Data is necessary for any of the following purposes:

- The prevention or detection of crime;
- The apprehension or prosecution of offenders;
- The assessment or collection of a tax or duty; or
- By order of a court or by any rule of law.

5.10. DATA PROTECTION TRAINING

5.10.1. All ClientEarth Employees and Employees of Third Parties (Data Processors) that have access to Personal Data will have their responsibilities under this policy outlined to them as part of their staff induction training. In addition, ClientEarth and Third Parties will provide regular Data Protection training and procedural guidance for their staff.

5.10.2. The training and procedural guidance set forth will consist of, at a minimum, the following elements:

- The Data Protection Principles set forth in Section 4.2 above.
- Each Employee's duty to use and permit the use of Personal Data only by authorised persons and for authorised purposes.
- The need for, and proper use of, the forms and procedures adopted to implement this policy.
- The correct use of passwords, security tokens and other access mechanisms.
- The importance of limiting access to Personal Data, such as by using password protected screen savers and logging out when systems are not being attended by an authorised person.
- Securely storing manual files, printouts and electronic storage media.
- How to use email securely, including information on how to detect a phishing email
- Proper disposal of Personal Data by using secure shredding facilities.
- Any special risks associated with particular departmental activities or duties.

5.11. INTERNATIONAL DATA TRANSFERS

5.11.1. ClientEarth will take all possible steps to avoid transferring Personal Data to internal or Third Party recipients located in a country outside the European Economic Area (EEA).

5.11.2. However, ClientEarth may transfer Personal Data to internal or Third Party recipients located in countries outside the EEA where an adequate transfer mechanism is in place, as detailed in Appendix A. This will include transfers to the U.S. on the basis of controller to controller Model Clause or the Privacy Shield mechanism in limited circumstances where necessary for Processing by ClientEarth or Third Parties.

5.11.3. In the case of other transfers to Third Party recipients located in countries outside the EEA, ClientEarth will take steps to ensure such transfers are limited to the minimum personal data necessary, that such transfers occur on an occasional basis, and that the relevant Personal Data is anonymised where necessary. Such circumstances may include transfers of Personal Data to hotels for the purposes of booking events and to Third Party funders located outside the EEA. Additionally, in such circumtances, ClientEarth will only transfer Personal Data where one of the transfer scenarios listed below applies:

- The Data Subject has given their Explicit Consent to the proposed transfer.
- The transfer is necessary for the performance of a contract with the Data Subject.
- The transfer is necessary for the implementation of pre-contractual measures taken in response to the Data Subject's request.
- The transfer is necessary for the conclusion or performance of a contract concluded with a Third Party in the interest of the Data Subject.
- The transfer is legally required on important public interest grounds.
- The transfer is necessary for the establishment, exercise or defence of legal claims.
- The transfer is necessary in order to protect the vital interests of the Data Subject.

5.12. TRANSFERS TO THIRD PARTIES

5.12.1. ClientEarth will only transfer Personal Data to, or allow access by, Third Parties for the purposes listed in Section 4.4.1.

5.12.2. ClientEarth will only transfer Personal Data to, or allow access by, Third Parties when it is assured that the information will be Processed legitimately and protected appropriately by the recipient. Where Third Party Processing takes place, ClientEarth will first identify if, under applicable law, the Third Party is considered a Data Controller or a Data Processor of the Personal Data being transferred.

5.12.3. Where the Third Party is deemed to be a Data Controller, ClientEarth will enter into an appropriate agreement with the Controller to clarify each party's responsibilities in respect to the Personal Data transferred.

5.12.4. Where the Third Party is deemed to be a Data Processor, will enter into an adequate Processing agreement with the Data Processor. The agreement must require the Data Processor to protect the Personal Data from further disclosure and to only Process Personal Data in compliance with ClientEarth instructions. In addition, the agreement will require the Data Processor to implement appropriate technical and organisational measures to protect the Personal Data, as well as procedures for providing notification of Personal Data Breaches.

5.12.5. When outsourcing services to a Third Party (including Cloud Computing services), ClientEarth will identify whether the Third Party will Process Personal Data on its behalf and whether the outsourcing will entail any Third Country transfers of Personal Data.

5.12.6. Regular audits of Processing of Personal Data performed by Third Parties, especially in respect of technical and organisational measures they have in place, should be undertaken. Any major deficiencies identified will be reported to and monitored by the ClientEarth Senior Management team.

5.13. COMPLAINTS HANDLING

5.13.1. Data Subjects with a complaint about the Processing of their Personal Data should put forward the matter in writing to **datarequests@clientearth.org**. An investigation of the complaint will be carried out to the extent that is appropriate based on the merits of the specific case. ClientEarth will inform the Data Subject of the progress and the outcome of the complaint within a reasonable period.

5.13.2. If the issue cannot be resolved through consultation with the Data Subject, then the Data Subject should be advised that they may, at their option, seek redress through mediation, binding arbitration, litigation, or via a complaint to the Information Commissioner's Office (ICO).

5.14. BREACH REPORTING

5.14.1. Any individual who suspects that a Personal Data Breach has occurred due to the theft or exposure of Personal Data must immediately notify the Security and Compliance officer or Head of Operations providing a description of what occurred. Notification of the incident can be made via e-mail to **databreach@clientearth.org** or by calling. The IT Manager should update the internal breach log, including pertinent facts relating to the incident, effects and remedial actions taken.

5.14.2. All reported incidents will be investigated to confirm whether or not a Personal Data Breach has occurred. For severe Personal Data Breaches, ClientEarth must inform the ICO within 72 hours of becoming aware of the breach. In some cases, affected Data Subjects should be advised of the personal data breach.

5.14.3. Guidance can be found in the Data Breach Incident Management Policy.

6. Policy Maintenance

6.1. PUBLICATION

6.1.1. This policy shall be available to all Employees through the ClientEarth Policy library on SharePoint. In the case of areas which employ non-desk based employees, then a hard copy will be made available in the staff area.

6.2. EFFECTIVE DATE

6.3. REVISIONS

7. Related Documents

- Incident Management Policy
- Data Retention Policy
- Records of Processing Activities
- Employee Handbook

Appendix A – Adequacy for Personal Data Transfers

The following is a list of countries recognised as having an adequate level of legal protection for the rights and freedoms of Data Subjects in relation to the Processing of their Personal Data:

- EU Countries (Austria, Belgium, Bulgaria, Croatia, Republic of Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden and the UK)
- Iceland
- Liechtenstein
- Norway
- Andorra
- Argentina
- Canada (commercial organisations)
- Faroe Islands
- Guernsey
- Israel
- Isle of Man
- Jersey
- New Zealand
- Switzerland
- Uruguay
- United States (Privacy Shield certified organisations)

The following are a list of countries that can provide adequate protection when transfers are made to countries lacking an adequate level of legal protection.

Appropriate Safeguards

- Model Clauses
- Binding Corporate Rules
- Codes of Conduct
- Certification Mechanisms

Derogations

- Explicit Consent
- Compelling Legitimate Interests
- Important reasons of Public Interest
- Transfers in response to a foreign legal requirement
- Data Protection Act approved contracts between Data Controllers and Data Processor