CONSEQUENCE UK LTD
PRIVACY POLICY MAY 2018

Introduction

Consequence UK is committed to protecting the rights and freedoms of data subjects and safely and securely processing their data in accordance with all of our legal obligations.

We hold personal data about our employees, clients, suppliers and other individuals for a variety of business purposes.

This policy sets out how we seek to protect personal data and ensure that our staff understand the rules governing their use of the personal data to which they have access in the course of their work.

The principles

Consequence UK Ltd shall comply with the principles of data protection (the Principles) enumerated in the EU General Data Protection Regulation. We will make every effort possible in everything we do to comply with these principles. The Principles are:

- **Lawful, fair and transparent** - Data collection must be fair, for a legal purpose, and we must be open and transparent as to how the data will be used.
- **Limited for its purpose** - Data can only be collected for a specific purpose.
- **Data minimisation** - Any data collected must be necessary and not excessive for its purpose.
- **Accurate** - The data we hold must be accurate and kept up to date.
- **Retention** - We cannot store data longer than necessary.
- **Integrity and confidentiality** - The data we hold w be kept safe and secure.

Lawful basis for processing data

Consequence UK Ltd must establish a lawful basis for processing data. Ensure that any data we are responsible for managing has a written lawful basis approved by the Data Protection Officer (DPO). At least one of the following conditions must apply whenever we process personal data:

- **Consent** - We hold recent, clear, explicit, and defined consent for the individual's data to be processed for a specific purpose.
- **Contract** - The processing is necessary to fulfil or prepare a contract for the individual.
- **Legal obligation** - We have a legal obligation to process the data (excluding a contract).
- **Vital interests** - Processing the data is necessary to protect a person's life or in a medical situation.
- **Public function** - Processing necessary to carry out a public function, a task of public interest or the function has a clear basis in law.
- **Legitimate interest** - The processing is necessary for our legitimate interests. This condition does not apply if there is a good reason to protect the individual's personal data which overrides the legitimate interest.

We will ensure that individuals whose data is being processed by Consequence UK are informed of the lawful basis for processing their data, as well as the intended purpose. This will apply whether we have collected the data directly from the individual, or from another source.

Responsibilities

Consequence UK responsibilities

- Analysing and documenting the type of personal data we hold
- Checking procedures to ensure they cover all the rights of the individual
- Identify the lawful basis for processing data
- Ensuring consent procedures are lawful
- Implementing and reviewing procedures to detect, report and investigate personal data breaches
- Store data in safe and secure ways
- Assess the risk that could be posed to individual rights and freedoms should data be compromised

Responsibilities of the Data Protection Officer (DPO)

- Keeping the Board updated about data protection responsibilities, risks and issues
- Reviewing all data protection procedures and policies on a regular basis
- Arranging data protection training and advice for all staff members and those included in this policy
- Answering questions on data protection
- Responding to individuals such as clients and employees who wish to know which data is being held on them by us
- Checking and approving with third parties that handle the company's data any contracts or agreement regarding data processing

Responsibilities of Consequence UK IT Support

- Ensure all systems, services, software and equipment meet acceptable security standards
- Checking and scanning security hardware and software regularly to ensure it is functioning properly
- Researching third-party services, such as cloud services the company is considering using to store or process data

Storing data securely

- In cases when data is stored on printed paper, it will be kept in a secure place where unauthorised personnel cannot access it
- Printed data will be shredded when it is no longer needed
- Data stored on a computer will be protected by strong passwords that are changed regularly.
- Data stored on CDs or memory sticks must be encrypted or password protected and locked away securely when they are not being used
- The DPO must approve any cloud used to store data and must be in line with regulations
- Servers containing personal data must be kept in a secure location, away from general office space
- Data should be regularly backed up in line with the company's backup procedures
- All servers containing sensitive data must be protected by security software
- All possible technical measures must be put in place to keep data secure

- If personal data is being viewed on a computer screen and the computer in question is to be left unattended for any period of time, the user must lock the computer and screen before leaving it;
- Deletion of electronbic copies of any personal data should be securely deleted.
- All electronic copies of personal data should be stored securely using passwords and data encryption;
- All emails containing personal data must be encrypted
- Personal data may be transmitted over secure networks only
- All passwords used to protect personal data should be changed regularly and should not use words or phrases that can be easily guessed or otherwise compromised. All passwords must contain a combination of uppercase and lowercase letters, numbers, and symbols. Under no circumstances should any passwords be written down
- Where personal data is to be sent by post or fax the recipient should be informed in advance of it being done and agreement made to how it is best done securely. All post will be sent by tracked delivery
- Personal data must be handled with care at all times and should not be left unattended for any period of time without securing it or on view at any time to a third party who does not need access to it;
- Personal data may only be transferred to devices belonging to associates or other parties working on behalf of consequence UK where the party in question has agreed to comply fully with Consequence GDPR Policy (They will have to demonstrate that all suitable technical and organisational measures have been taken to comply);
- Paper copies, along with any electronic copies stored on physical, removable media should be stored securely in a locked drawer, cabinet or office;
- Deletion of hardcopy data should be securely deleted from any external devices and disposed of and paper copies shredded securely deleted and disposed of

Data retention

We will retain personal data for no longer than is necessary. What is necessary will depend on the circumstances of each case, taking into account the reasons that the personal data was obtained, but should be determined in a manner consistent with our data retention guidelines.

Transferring data internationally

Consequence UK will not transfer personal data abroad, or anywhere else outside of normal rules and procedures without express permission from the client

Rights of individuals

Individuals have rights to their data which we will respect and comply with to the best of our ability. We will ensure individuals can exercise their rights in the following ways:

- Right to be informed
- Right of access
- Right to rectification
- Right to erasure
- Right to restrict processing
- Right to data portability
- Right to object
- Rights in relation to automated decision making and profiling

Privacy notices

A privacy notice must be supplied at the time the data is obtained if obtained directly from the data subject. If the data is not obtained directly from the data subject, the privacy notice must be provided within a reasonable period of having obtained the data, which mean within one month. If the data is being used to communicate with the individual, then the privacy notice will be supplied at the latest when the first communication takes place.

The following information must be included in a privacy notice to all data subjects:

- The purpose of processing the data and the lawful basis for doing so
- The legitimate interests of the controller or third party, if applicable
- The right to withdraw consent at any time, if applicable
- The source of the personal data, and whether it came from publicly available sources (only for data not obtained directly from the data subject)
- Access to the company's policy

Data Subject Access Requests

An individual has the right to receive confirmation that their data is being processed, access to their personal data and supplementary information which means the information which should be provided in a privacy notice.

How we deal with subject access requests

We will provide an individual with a copy of the information the request, free of charge. This must occur without delay, and within one month of receipt. We endeavour to provide data subjects access to their information in commonly used electronic formats, and where possible, provide direct access to the information through a remote accessed secure system.

We can refuse to respond to certain requests, and can, in circumstances of the request being manifestly unfounded or excessive, charge a fee. If the request is for a large quantity of data, we can request the individual specify the information they are requesting.

Right to erasure

Individuals have a right to have their data erased and for processing to cease in the following circumstances:

- Where the personal data is no longer necessary in relation to the purpose for which it was originally collected and / or processed
- Where consent is withdrawn
- Where the individual objects to processing and there is no overriding legitimate interest for continuing the processing
- The personal data was unlawfully processed or otherwise breached data protection laws
- To comply with a legal obligation
- The processing relates to a child

We can only refuse to comply with a right to erasure in the following circumstances:

- To exercise the right of freedom of expression and information
- To comply with a legal obligation for the performance of a public interest task or exercise of official authority
- For public health purposes in the public interest
- For archiving purposes in the public interest, scientific research, historical research or statistical purposes
- The exercise or defence of legal claims

If personal data that needs to be erased has been passed onto other parties or recipients, they will be contacted and informed of their obligation to erase the data.

The right to object

Individuals have the right to object to their data being used on grounds relating to their particular situation. We will cease processing unless:

- We have legitimate grounds for processing which override the interests, rights and freedoms of the individual.
- The processing relates to the establishment, exercise or defence of legal claims.

We will always inform the individual of their right to object at the first point of communication, i.e. in the privacy notice. We must offer a way for individuals to object online.

The right to restrict automated profiling or decision making
We may only carry out automated profiling or decision making that has a legal or similarly significant effect on an individual in the following circumstances:

- It is necessary for the entry into or performance of a contract.
- Based on the individual's explicit consent.
- Otherwise authorised by law.

In these circumstances, we must:

- Give individuals detailed information about the automated processing.
- Offer simple ways for them to request human intervention or challenge any decision about them.
- Carry out regular checks and user testing to ensure our systems are working as intended.

Using third party controllers and processors

As a data controller and/or data processor, we will have written contracts in place with any third-party data controllers and/or data processors that we use. The contract will contain specific clauses which set out our and their liabilities, obligations and responsibilities.

As a data controller, we will only appoint processors who can provide sufficient guarantees under GDPR and that the rights of data subjects will be respected and protected.

As a data processor, we ensure that we only act on the documented instructions of a controller and acknowledge their responsibilities as a data processor under GDPR and will protect and respect the rights of data subjects.

Audits, monitoring and training

We will audit our data and associated risk on a yearly basis - This contains information on what data is held, where it is stored, how it is used, who is responsible and any further regulations or retention timescales that may be relevant.

- **Monitoring** - Everyone is the organisation must comply fully with GDPR regulations and is responsible for comply with this policy fully and at all times.
- **Training** - All employees will receive adequate training on provisions of data protection law specific for their role.

Reporting breaches

Any breach of this policy or of data protection laws must be reported as soon as practically possible. This means as soon as we have become aware of a breach it must be reported. Consequence has a legal obligation to report any data breaches within 72 hours.