Beck & Pollitzer

General Data Protection Policy

Policy Introduction

This policy aims to set out our procedures in relation to the General Data Protection Regulations (GDPR) at an organisational level within Beck & Pollitzer ("we"). As such, this policy outlines Beck & Pollitzer procedures relating to the obtaining, maintaining, processing and destroying of personal data. Beck & Pollitzer has a duty of care to ensure that all its practices are safe, compliant and protect personal data. We are committed to safety and its processes are designed to protect those whose personal information it holds. This policy also sets out how we aim to protect personal data and ensure that this is implemented across the breadth of employment activities. Beck & Pollitzer holds personal data about its employees, job applicants, customers, suppliers, sub-contractors and other third parties. Beck & Pollitzer complies with current data protection legislation when obtaining, maintaining and destroying personal data.

Policy Scope

The scope of this policy covers:

- all processing activities involving personal and sensitive personal data where Beck & Pollitzer acts as the Data Controller, regardless of the media on which that data is stored,
- all Employees, Contractors, Sub-Contractors, Third Parties, Processors, or others who process Personal or Sensitive personal Data on behalf of Beck & Pollitzer
- all geographic territories where Beck & Pollitzer operates. All Beck & Pollitzer affiliates and its employees must process personal data with due diligence and in compliance with the statutory requirements and this policy.

Definitions of Data Protection Terms

- Data Subject is a living, identified or identifiable individual about whom Beck & Pollitzer holds personal data (e.g. Beck & Pollitzer's employees, subcontractor's employees, customer, supplier, etc.).
- Personal data is any information identifying a data subject or information relating to a data subject that can be identified (directly or indirectly) from that data alone or in combination with other identifiers Beck & Pollitzer possess or can reasonably access.
- General Data Protection Regulation (GDPR) is a legal framework for the collection and processing of personal information of individuals.
- Data controller is the person or organisation that determines when, why and how to process personal data. It is responsible for establishing practices and policies in line with the GDPR.
- Data Protection Officer (DPO) is responsible for ensuring that their organisation processes the personal data of its staff, customers, providers or any other individuals (also referred to as data subjects) in compliance with the applicable data protection rules. Contact: dpo@beck-pollitzer.com
- Data Processing of personal data means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. Processing also includes transferring personal data to third parties.
- Consent is agreement which must be freely given, specific, informed and be an unambiguous indication of the data subject's wishes by which they, by a statement or by a clear positive action, signify agreement to the processing of personal data relating to them.
- Personal data breach is any act or omission that compromises the security, confidentiality, integrity or availability of personal data or the physical, technical, administrative or organisational safeguards that Beck & Pollitzer put in place to protect it. The loss, unauthorised access, disclosure or acquisition of personal data is a personal data breach.

Data Protection Principles

The GDPR sets out principles regarding the use of personal data that set the framework upon which data processing activities are conducted. As such, all personal data must:

- Be processed lawfully, fairly and in a transparent manner.
- Be collected for a specific, explicit and legitimate purpose and not further processed in a manner which is incompatible with that purpose.
- Be adequate, relevant, and limited for what is necessary in relation to the purposes for which it is processed.

- Be accurate and where necessary, kept up to date. Every reasonable step must be taken to ensure that personal data that are inaccurate are erased and rectified without delay whilst having regard to the purposes for which they are processed.
- 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 are processed.
- 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, using appropriate technical or organisational measures.

Beck & Pollitzer must have relevant procedures in place in order to demonstrate accountability and compliance with each of the above principles which are set out in the General Data Protection Regulation EU2016/679 applicable since May 2018. We are responsible for and must be able to demonstrate compliance with the data protection principles listed above ('accountability').

Employee Responsibilities

Training will be given on the requirements of the GDPR; Employees are required to complete all assigned data protection training as requested. Employees must adhere to the following responsibilities at all times during the course of their employment:

- Understand the data protection obligations fully and make sure that they are continuously mindful of these throughout the course of their employment activities.
- Ensure that all data processing activities they are undertaking comply with Beck & Pollitzer procedures and are justified.
- Do not use data in any unlawful manner or in any manner which contradicts this policy.
- Store all data correctly, all data should be kept secure and protected from any unlawful processing and against accidental loss or destruction.
- Hold data for the required length of time only and in light of the purposes for which that data was originally collected, held and processed.
- Comply with this procedure at all times.
- If they become aware of any data breaches or near misses or if they have any concerns relating to data, they must raise this immediately with the Data Protection Officer or equivalent or a member of management. Employees should be vigilant regarding information and report anything which is contradictory to Beck & Pollitzer procedures.

Individual Rights under GDPR

Data subjects have the following rights under GDPR:

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

Lawfulness, Fairness and Transparency

Beck & Pollitzer may only collect, process and share personal data fairly and lawfully and for specified purposes. The GDPR restricts our actions regarding personal data to specified lawful purposes. These restrictions are not intended to prevent processing, but ensure that we process personal data fairly and without adversely affecting the data subject. The GDPR allows processing for specific purposes, some of which are set out below:

- the processing is necessary for the performance of a contract with the data subject.
- to meet legal compliance obligations.
- to pursue legitimate interests for purposes where they are not overridden because the processing prejudices the interests or fundamental rights and freedoms of data subjects.
- to protect the data subject's vital interests.
- the data subject has given their consent where applicable.

The GDPR requires data controllers to provide detailed, specific information to data subjects regardless of whether the information was collected directly from data subjects or from elsewhere. The information must be provided through appropriate privacy notices. A data controller must only process personal data on the basis of one or more of the lawful bases set out in the GDPR, which include consent.

A data subject consents to processing of personal data, if they indicate agreement clearly either by a statement or positive action to the processing. Consent requires affirmative action so silence, pre-ticked boxes or inactivity are unlikely to be sufficient. When processing special category data or criminal convictions data, Beck & Pollitzer will usually rely on a legal basis for processing other than explicit consent or consent if possible. Such information is not only to meet the our legal responsibilities but, for example, for purposes of personal management and administration, suitability for employment and to comply with equal opportunities legislation.

Whenever Beck & Pollitzer collect personal data directly from data subjects, including for human resources or employment purposes, we must provide the data subject with all the information required by the GDPR including the identity of the controller and how and why we will use, process, disclose, protect and retain that personal data through a privacy notice.

Purpose Limitation

Personal data must be collected only for specified, explicit and legitimate purposes. It must not be further processed in any manner incompatible with those purposes. We cannot use personal data for new, different or incompatible purposes from that disclosed when it was first obtained unless Beck & Pollitzer has informed the data subject of the new purposes and explained the legal basis for doing so.

Data Minimisation

Personal data must be adequate, relevant, and limited to what is necessary in relation to the purposes for which it is processed. Beck & Pollitzer must ensure any personal data collected is adequate and relevant for the intended purposes and ensure that when personal data is no longer needed for specified purposes, it is deleted or anonymised in accordance with our data retention guidelines.

Accuracy

Personal data must be accurate and, where necessary, kept up to date. It must be corrected or deleted without delay when inaccurate. Beck & Pollitzer must take all reasonable steps to destroy or amend inaccurate or out-of-date personal data.

Store Limitation

Beck & Pollitzer must not keep personal data in a form which permits the identification of the data subject for longer than needed for the legitimate business purpose or purposes for which it was originally collected for.

Beck & Pollitzer will maintain retention guidelines to ensure personal data is deleted after a reasonable time for the purposes for which it was being held, unless a law requires that data be kept for a minimum time. Beck & Pollitzer must take all reasonable steps to destroy or erase from its systems all personal data that it no longer requires in accordance with all our applicable records and retention policies. This includes requiring third parties to delete that data where applicable.

Security, Integrity and Confidentiality

Personal data must be secured by appropriate technical and organisational measures against unauthorised or unlawful processing, and against accidental loss, destruction or damage. 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. Beck & Pollitzer is responsible for ensuring that any personal data that it holds and/or processes as part of a job role is stored securely.

Beck & Pollitzer must ensure that personal information is not disclosed either orally or in writing, or via web pages, or by any other means, accidentally or otherwise, to any unauthorised third party. Employees should note that unauthorised disclosure may result in action under the disciplinary procedure, which may include summary dismissal for gross misconduct. Electronic data should be coded, encrypted, or password protected both on a local hard drive and on a network drive that is regularly backed up. If a copy is kept on removable storage media, that media must itself be kept in a secure filing cabinet, drawer, or safe.

When an employee is travelling with a device containing personal data, they must ensure both the device and data is password protected. Employees should avoid travelling with hard copies of personal data where there is secure electronic storage available. If an employee is travelling with either an electronic device or with hard copies of personal data, these should be kept securely in a bag and where possible locked away out of sight i.e. in the boot of a car.

Accountability

The data controller must implement appropriate technical and organisational measures in an effective manner, to ensure compliance with data protection principles. The data controller is responsible for, and must be able to demonstrate, compliance with the data protection principles.

Reporting a Personal Data Breach

A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored, or processed.

The following are examples of data breaches:

a) Access by an unauthorised third party.
b) Deliberate or accidental action (or inaction) by a data controller or data processor.
c) Sending personal data to an incorrect recipient.
d) Computing devices containing personal data being lost or stolen.
e) Alteration of personal data without permission.
f) Loss of availability of personal data.

If an employee knows or suspects that a personal data breach has occurred, they should not attempt to investigate the matter themselves. They should instead immediately contact the Data Protection Officer (dpo@beck-pollitzer.com) who is designated as the key point of contact for personal data breaches. In the event Beck & Pollitzer become aware of a breach, or a potential breach, an investigation will be carried out by the Data Protection Officer or equivalent.

Beck & Pollitzer will notify the relevant authority of a breach which is likely to pose a risk to people's rights and freedoms without undue delay and at the latest within 72 hours of discovery. If we are unable to report in full within this timescale, an initial report will be compiled to the relevant authority, and this will be followed by a full report in more than one instalment if so required.

Beck & Pollitzer will undertake to notify the individual whose data is the subject of a breach if there is a high risk to people's rights and freedoms without undue delay and may, dependent on the circumstances, be made before the supervisory authority is notified.

Beck & Pollitzer records all personal data breaches regardless of whether they are notifiable or not as part of its general accountability requirement under the Data Protection Act 2018. It records the facts relating to the breach, its effects and the remedial action taken.

Data Subjects Rights and Requests

Data subjects have rights when it comes to how Beck & Pollitzer handles their personal data.

These include rights to:

- withdraw consent to processing at any time.
- request access to their personal data that Beck & Pollitzer hold.
- prevent Beck & Pollitzer use of their personal data for direct marketing purposes.
- ask us 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.
- restrict processing in specific circumstances.
- challenge processing which has been justified on the basis of Beck & Pollitzer legitimate interests or in the public interest.
- be notified of a personal data breach which is likely to result in high risk to their rights and freedoms.
- make a complaint to the supervisory authority.
- in limited circumstances, receive or ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format.

Sharing Personal Data

Beck & Pollitzer are not allowed to share personal data with third parties unless certain safeguards and contractual arrangements have been put in place. Beck & Pollitzer may only share the personal data it holds with another employee or representative of Beck & Pollitzer if the recipient has a job-related to this employee and need to know the information.

Training and Audit

Beck & Pollitzer are required to ensure all employees have undergone adequate training to enable them to comply with data protection and privacy laws. We must also regularly test our systems and processes to assess compliance.

Failure to Comply with the GDPR Guidelines

Beck & Pollitzer takes its responsibility to protect personal data extremely seriously and as such organisational compliance to current data protection legislation is of the highest importance. Failure to comply with Beck & Pollitzer data protection policies and procedures puts both the organisation and employees at risk. Failure to comply with any requirement may lead to disciplinary action.

If any employees, clients, third party organisations or stakeholders or others have any concerns or questions regarding Beck & Pollitzer stance on the protection of personal data or this policy, please do not hesitate to contact Data Protection Officer or equivalent representative.

Subject Access Request

If an employee wishes to access the personal data which we hold about them, they must make a request in writing to the Data Protection Officer or an equivalent representative.

Beck & Pollitzer will respond to the request without delay and at latest, within one month of receiving the written request. If necessary, this timescale can be extended by a further two months if the request is complex. However, the employee will be contacted within one month of the receipt of the request and we will explain why an extension is necessary in this instance.

Beck & Pollitzer will endeavour to provide the information in a commonly used electronic format. Some information may be exempt from subject access requests, in such instances, the Data Protection Officer or equivalent will explain the reasons why this request will not be carried out.

Changes to this Policy

Beck & Pollitzer reserve the right to change this policy at any time. We last revised this policy on May 2024.

Simon Harris
Chief Financial Officer