BNEI AKIVA
UNITED KINGDOM

Data Protection Policy

Storing, Working with and Destroying records

Context & Overview

Key Details

Policy prepared by: Adam Waters
Approved on: May 25th 2018
Next review: May 25th 2019

Introduction

Bnei Akiva UK and Friends of Bnei Akiva (BACHAD) henceforth known as "Bnei Akiva", need to gather and use certain information about individuals. This can include customers, suppliers, business contacts, employees, and other people Bnei Akiva has a relationship with or may need to contact.

Bnei Akiva processes and uses this information, under the lawful basis of consent, contract, legitimate interest and/or legal obligation.

This policy describes how this personal data must be collected, handled and stored to meet Bnei Akiva's data protection standards – and to comply with the law.

Why this policy exists

This data protection policy ensures Bnei Akiva:

- Complies with data protection n law and follows good practice
- Protects the rights of staff, customers, and partners
- Is open about how it stores and processes individuals data
- Protects itself from risks of data breach.

Data Protection Law

The Data Protection Act 1998, and the General Data Protection Regulations (GDPR), describe how organisations must collect, handle and store personal information.

These rules apply regardless of whether data is stored electronically, on paper, or on other materials.

Article 5 of the GDPR requires that personal date be:

1. Processed lawfully, fairly and in a transparent manner
2. Collected for specific, explicit and legitimate purposes, and not further processed in a manner that is incompatible with these purposes.
3. Adequate, relevant and limited to what is nexessary
4. Accurate, and where necessary, kept up to date
5. Is not kept longer than necessary for the purpose for which the data was processed
6. Processed in a manner that ensures appropriate security

Policy Scope

This policy applies to:

- The Bnei Akiva Batim (offices)
- All local branches of Bnei Akiva in the UK (Svivot)
- All staff or volunteers
- All contractors, suppliers, and other people working on behalf of Bnei Akiva

It applies to all data that Bnei Akiva holds relating to identifiable individuals, even if that information technically falls outside of the relevant legislation. This can include:

- Names of individuals
- Postal addresses
- Email addresses
- Telephone Numbers
- Medical information
- Financial information

Bnei Akiva recognizes the rights of the individual as set out in the GDPR legislation, which are:

- 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 related to automated decision making including profiling

Data Protection Risks

This policy helps to protect Bnei Akiva from some very real data security risks, including:

- Breaches of confidentiality. For instance, information being given out innapropriately
- Failing to offer choice. For instance, all individuals should be free to choose how Bnei Akiva uses data relating to them
- Reputational Damage. For instance, Bnei Akiva and the individuals it works with could suffer if hackers successfully gained access to sensitive data.

Responsibilities

Everyone who works for or with Bnei Akiva has some responsibility for ensuring data is collected, stored and handled appropriately. Each team that handles data must ensure that it is handled and processed in line with this policy and data protection principles. The following people have key area of responsibility:

- The COO, on behalf of the trustees of Friend of Bnei Akiva (BACHAD), is responsible for ensuring that Bnei Akiva meets its legal obligations. The COO will act as the data protection officer and is responsible for:

- Keeping the trustees and National Director updated on any data protection risks and responsibilities.
- Reviewing all data protection procedures and policies in line with an agreed schedule.
- Arranging any training necessary for staff covered by this policy.
- Handling data protection questions from staff or anyone covered by this policy.
- Dealing with requests from individuals to see the data Bnei Akiva holds about them.
- Checking and approving any contracts with third parties that may handle sensitive data.
- Ensuring all systems, services and equipment used for storing data meet acceptable security standards
- Evaluating any third party services Bnei Akiva is using to store data, e.g. cloud computing software
- Approving any data protection statements attached to communications such as emails and letters.
- Where necessary, working with other staff to ensure marketing initiatives abide by data protection principles

General Staff Guidelines

The only people able to access data covered by this policy should be those who **need it for their work**.

Data **should not be shared informally**. When access of confidential information is required, employees can request it from their line managers.

Employees should keep all data secure, by taking sensible precautions and following the guidelines below.

In particular, **strong passwords must be used** and they should never be shared

Personal data **should not be disclosed** to unauthorised people, either within the company or externally.

Data should be **regularly reviewed and updated** if it is found to be out of date. If on longer required, it should be deleted and disposed of.

Employees **should request help** from their line manager, or the COO, if they are unsure about any aspect of data protection.

Data Storage

When data is stored on paper, it should be kept in a secure place where unauthorised people cannot see it.

- When not required, the paper or files should be kept in a locked drawer or filing cabinet.
- Employees should ensure no print outs with data are left where unauthorised people might see them, e.g. a desk, or the printer
- Data printouts should be shredded and disposed of securely when no longer required.

When data is stored electronically, it should be protected from unauthorised access, accidental deletion, and malicious hacking attempts:

- Data should be protected by strong passwords that are changed regularly
- If data is stored on removable media (e.g. USB/Hardrive) these should be kept locked away securely when not being used.
- Data should only be stored on the designated drives and servers, and approved cloud computing services
- Data should be backed up frequently
- All servers and computers containing data should be protected by approved security software and a firewall.

Data Use

It is when personal data is accessed and used that it is at the greatest risk of loss, corruption and theft. Therefore:

- When working with personal data, employees should ensure the screens of their computer are locked when left unattended.
- Personal data should not be shared informally. In particular, it should never be sent by email
- Data must be encrypted before being transferred electronically.
- Employees should not save copies of personal data to their own computers.

Data Accuracy

The law requires Bnei Akiva takes reasonable steps to ensure data is kept accurate and up to date. Therefore:

- Data will be held in as few places as possible. Staff should not create any unnecessary data sets.
- Staff should take every opportunity to ensure data is updated. For instance, by confirming a customer's details when they call.
- Data should be updated as inaccuracies are discovered. For example, if a customer can no longer be reached on their stored telephone number, it should be removed from the database.

Subject Access Requests

All individuals who are the subject of personal data held by Bnei Akiva are entitled to:

- Ask what information the company holds about them and why
- Ask how to gain access to it

- Be informed how to keep it up to date
- Be informed how the company is meeting its data protection obligations

If an individual contacts the company requesting this information, this is called a subject access request (SAR). These should be made via email to operations@bauk.org, or by calling 0208 209 1319 ext.#. The data controller will always verify the identity of anyone making a subject access request before handing over any information.

Providing Information

Bnei Akiva aims to ensure that individuals are aware their data is being processed, and that they understand:

- How their data is being used
- How to exercise their rights

Employees should refer to their employee agreement for further guidelines in regards to emails, IT systems and Social Media policies.

Record Retention and Destruction Policy

Purpose

The purpose of this Policy is to ensure that necessary records and documents are adequately protected and maintained and to ensure that records that are no longer needed by Bnei Akiva UK, or are of no value, are discarded at the proper time. This Policy is also for the purpose of aiding employees of Bnei Akiva UK in understanding their obligations in retaining electronic documents - including e-mail, Web files, text files, sound and movie files, PDF documents, and all Microsoft Office or other formatted files.

Policy

This Policy represents Bnei Akiva's policy regarding the retention and disposal of records and the retention and disposal of electronic documents.

Administration

Attached as Appendix A is a Record Retention Schedule that is approved as the initial maintenance, retention and disposal schedule for physical records of Bnei Akiva and the retention and disposal of electronic documents. The Chief Operating Officer (the "COO") is the officer in charge of the administration of this Policy and the implementation of processes and procedures to ensure that the Record Retention Schedule is followed.

Suspension of Record Disposal in Event of Litigation or Claims

In the event Bnei Akiva UK is served with any legal request for documents or any employee becomes aware of a governmental investigation or audit concerning Bnei Akiva UK or the commencement of any litigation against or concerning Bnei Akiva UK, such employee shall inform the COO and any further disposal of documents shall be suspended until shall time as the COO, with the advice of counsel, determines otherwise. The COO shall take such steps as is necessary to promptly inform all staff of any suspension in the further disposal of documents.

Applicability

This Policy applies to all physical records generated in the course of Bnei Akiva UK's operation, including both original documents and reproductions. It also applies to the electronic documents described above.

APPENDIX A - RECORD RETENTION SCHEDULE

A. Accounting and Finance

Record Type	Retention Period
Accounts Payable ledgers and schedules	7 years
Accounts Receivable ledgers and schedules	7 years
Annual Audit Reports and Financial Statements	Permanent
Annual Audit Records, including work papers and other documents that relate to the audit	7 years after completion of audit
Annual Plans and Budgets	7 years
Bank Statements and Canceled Checks	Permanent
Employee Expense Reports	7 years
General Ledgers	Permanent
Credit card records (documents showing customer credit card number)	7 years

Credit card record retention and destruction

All records showing customer credit card number must be locked in a desk drawer or a file cabinet when not in immediate use by staff.

If it is determined that information on a document, which contains credit card information, is necessary for retention beyond 2 years, then the credit card number will be cut out of the document.

B. Participants Data

Record Type	Retention Period
Names	10 Years Post Participation
Email Address	10 Years Post Participation
Postal Address	10 Years Post Participation
Telephone Number	10 Years Post Participation
Medical Details	10 Years Post Participation
Administration of First Aid, Medication or Hospital/Doctor Visits	50 Years Post Participation
Disclosure or Safeguarding Information	50 Years Post Participation

C. Correspondence and Internal Memoranda

General Principle: Most correspondence and internal memoranda should be retained for the same period as the document they pertain to or support. For instance, a letter pertaining to a

particular contract would be retained as long as the contract (7 years after expiration). It is recommended that records that support a particular project be kept with the project and take on the retention time of that particular project file.

Correspondence or memoranda that do not pertain to documents having a prescribed retention period should generally be discarded sooner. These may be divided into two general categories:

1. Those pertaining to routine matters and having no significant, lasting consequences should be discarded *within two years.* Some examples include:

    - Routine letters and notes that require no acknowledgment or follow-up, such as notes of appreciation, congratulations, letters of transmittal, and plans for meetings.
    - Form letters that require no follow-up.
    - Letters of general inquiry and replies that complete a cycle of correspondence.
    - Letters or complaints requesting specific action that have no further value after changes are made or action taken (such as name or address change).
    - Other letters of inconsequential subject matter or that definitely close correspondence to which no further reference will be necessary.
    - Chronological correspondence files.

    Please note that copies of interoffice correspondence and documents where a copy will be in the originating department file should be read and destroyed, unless that information provides reference to or direction to other documents and must be kept for project traceability.

2. Those pertaining to non-routine matters or having significant lasting consequences should generally be retained permanently.

D. ELECTRONIC DOCUMENTS

1. **Electronic Mail**: Not all email needs to be retained, depending on the subject matter.
    - All e-mail—from internal or external sources—is to be deleted after 12 months.
    - Staff will strive to keep all but an insignificant minority of their e-mail related to business issues.
    - Staff will not store or transfer Bnei Akiva UK related e-mail on non-work-related computers except as necessary or appropriate for Bnei Akiva UK purposes.
    - Staff will take care not to send confidential Bnei Akiva UK information to outside sources.
    - Any e-mail staff deems vital to the performance of their job should be copied to the staff's server, and printed and stored in the employee's workspace.

2. Electronic Documents: including Microsoft Office Suite and PDF files. Retention also depends on the subject matter.

- **PDF documents** – The length of time that a PDF file should be retained should be based upon the content of the file and the category under the various sections of this policy. The maximum period that a PDF file should be retained is 7 years. PDF files the employee deems vital to the performance of his or her job should be printed and stored in the employee's workspace.
- **Text/formatted files** - Staff will conduct annual reviews of all text/formatted files (e.g., Microsoft Word documents) and will delete all those they consider unnecessary or outdated. After five years, all text files will be deleted from the network and the staff's desktop/laptop. Text/formatted files the staff deems vital to the performance of their job should be printed and stored in the staff's workspace.

3. Web Page Files: Internet Cookies

- All workstations: Internet browsers should be scheduled to delete Internet cookies once per month.

Bnei Akiva UK does not automatically delete electronic files beyond the dates specified in this Policy. It is the responsibility of all staff to adhere to the guidelines specified in this policy.

In certain cases a document will be maintained in both paper and electronic form. In such cases the official document will be the electronic document.

E. GRANT/DONATION RECORDS

Record Type	Retention Period
Original grant proposal	7 years after completion of grant period
Grant agreement and subsequent modifications, if applicable	7 years after completion of grant period
Final grantee reports, both financial and narrative	7 years after completion of grant period
All evidence of returned grant funds	7 years after completion of grant period
All pertinent formal correspondence including opinion letters of counsel	7 years after completion of grant period
Donor records and personal details	7 years are donation
Potential Donor Database records	2 years if no donation

F. PAYROLL DOCUMENTS

Record Type	Retention Period
Employee Expenses	4 years after termination

Record Type	Retention Period
Payroll Deductions	Termination + 7 years
Employee P45 – P60	Termination + 7 years
Payroll Registers (gross and net)	7 years

G. PENSION DOCUMENTS AND SUPPORTING EMPLOYEE DATA

General Principle: Pension documents and supporting employee data shall be kept in such a manner that Donors Forum can establish at all times whether or not any pension is payable to any person and if so the amount of such pension.

Record Type	Retention Period
Retirement and Pension Records	Permanent

H. PERSONNEL RECORDS

Record Type	Retention Period
Commissions/Bonuses/Incentives/Awards	7 years
Employee Earnings Records	Separation + 7 years
Employee Handbooks	1 copy kept permanently
Employee Medical Records	Separation + 6 years
Employee Personnel Records (including individual attendance records, application forms, job or status change records, performance evaluations, termination papers, withholding information, garnishments, test results, training and qualification records)	6 years after separation
Employment Contracts – Individual	7 years after separation
Employment Records - All Non-Hired Applicants (including all applications and resumes - whether solicited or unsolicited, results of post-offer, pre-employment physicals, results of background investigations, if any, related correspondence)	2-4 years (4 years if file contains any correspondence which might be construed as an offer)
Job Descriptions	3 years after superseded

I. TAX RECORDS

General Principle: Donors Forum must keep books of account or records as are sufficient to establish amount of gross income, deductions, credits, or other matters required to be shown in any such return.

These documents and records shall be kept for as long as the contents thereof may become material in the administration of federal, state, and local income, franchise, and property tax laws.