Allergy UK Data Protection Policy

Reference:	Data Protection Policy
Document Type:	Policy
Document Status:	Final
Owner:	Chief Executive
Review Period:	Annual
Next Review Date:	May 2019

Contents

3.5 Principle 5: Retaining data

3.5.1 Ensuring that information which is no longer in use is destroyed as soon as possible

3.6 Principle 6: Information security

3.6.1 Ensure data controllers establish measures which will prevent harm to the individual as a result of their information falling into the wrong hands

4. General Principles

4.1 Rights of individuals

4.1.1 Ensure that data controllers are clear on the rights of individuals when dealing with their data

4.2 Understand individuals' rights for direct marketing

4.3 Transfer of data abroad (outside the EU)

4.3.1 Ensure that all individuals' data is kept safe when travelling abroad

5. Contacting us

1. Document History

1.1 Document Location

This document can be accessed from the following location: www.allergyuk.org/other-gdpr-polices

1.2 Revision History

Revision Date:	First Version May 2018
Author:	Carla Jones, CEO
Version:	1.0
Summary of Changes:	

1.3 Approvals

This document requires the following approvals:

Name:	BAF Board
Job Title:	Trustees
Date of Approval:	22nd May 2018

2. Data Protection and Access to Information

In addition to the Data Protection and Access to Information part of the Employee Handbook, Allergy UK must also recognise the protection of data collected and held for non-Allergy UK individuals. These individuals could encompass:

1. Those living with allergy
2. Relatives or carers for those living with allergy
3. Event Attendees
4. Healthcare Professionals
5. Donors
6. Fundraisers
7. Corporate Partners
8. Manufacturers
9. Press Contacts
10. Persons signing-up to Allergy UK materials (E-News, Allergy Alerts etc.)
11. Other individuals of which Allergy UK has personal data

Allergy UK will comply with all statutory requirements of the General Data Protection Regulations 2018 (GDPR). The GDPR gives individuals the right to be aware of, seek access to, and have some control over, the nature and content of information held in relation to them by us, and to know the reasons why the information is being held or processed.

It is also each staff member responsibility to protect confidential sensitive information and personal data of individuals detailed above and any others that may be in contact with Allergy UK. This applies to information held on computer (either software programmes or electronic documents) or in a manual filing system.

Any person processing personal data must comply with the principles of good practice. Data must be:

- fairly and lawfully processed
- processed for limited purposes
- adequate, relevant and not excessive
- accurate
- not kept longer than necessary
- secure

Processing is any activity that involves use of the data, e.g. obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transferring personal data to third parties.

In addition to the six principles of good practice, the GDPR provides that any data must be processed in accordance with the data subject's rights and must not be transferred to non-EU countries without adequate protection.

Key changes that the GDPR introduces for charities include:

- More rigorous requirements for obtaining consent for collecting data
- Raising the age of consent for collecting an individual's data, which the draft Data Protection Bill indicates the UK will opt for 13 and over.
- Requiring a charity to delete data if it is no longer used for the purpose it was collected
- Requiring a charity to delete data if the individual revokes consent for the charity to hold the data (in cases where the individual has consented)
- Requiring charities to notify the relevant data protection authority of some data breaches within 72 hours of learning about the breach.

These new requirements will be detailed in each of the six principles of good practice found within this document. For the duration of this document, all policies detailed below which mention "individual(s)" will mean any individual type detailed at the beginning of this document, regardless of what team/department hold this data. The term "data controller(s)" will be used for any member of Allergy UK staff that has access, updates or holds "individuals" data.

3. Six Principles

3.1 Principle 1: Handling data fairly and lawfully

3.1.1. Ensure data controllers process data fairly

Data controllers must ensure that they tell individuals how their personal data will be used, in particular:

a) Who you are/Allergy UK is
b) What Allergy UK will use their information for, and
c) Anything else necessary to ensure Allergy UK is using their information fairly, including whether you plan to pass individuals details to other data controllers (internally or externally) and how you will contact people (phone, post, email etc.)

This must be done prior to using, storing, recording etc. their data.

3.1.2 Ensure data controllers do not do anything unlawful with the data:

Such as disclosing data that was given to data controllers in confidence.

3.1.3 Ensure that data controllers can satisfy at least one of the following conditions and notifies the condition to the individual

a) The individual has consented to the processing
b) The processing is necessary in relation to an arrangement or contract the individual has entered into or because the individual has asked for something to be done so that the action relating to that arrangement or contract can be completed (i.e. signed up for allergy alerts)
c) The processing is necessary because of a legal obligation that applies to Allergy UK
d) The processing is in Allergy UK's legitimate interests and is not prejudicial to the rights and freedoms of the individual.

3.1.4 Ensure data controllers have satisfied at least one of the criteria of the legal basis for processing if processing "sensitive personal data" or "special categories of data" and that this legal basis is notified to the individual

Sensitive Personal Data or special categories can be classified as:

a) The racial or ethnic origin of the individual
b) The individual's political opinions
c) The individual's religious beliefs or beliefs of a similar nature
d) Whether the individual is a member of a trade union
e) Information on the individual's physical or mental health condition
f) Information on the individual's sexual life
g) The commission or alleged commission of an offence by the individual, and
h) Information relating to the commission or alleged commission of an offence by the individual (i.e. the sentence of a court in relation to an offence).

There are times when data controllers within Allergy UK will deal with a *subject's physical health condition*. Therefore, in those cases, one of the following criteria must be adhered to:

a) The individual who the sensitive personal data is about has given explicit consent to the processing
b) The individual has deliberately made the information public
c) The processing is necessary for medical purposes and is undertaken by a health professional or by someone who is subject to an equivalent duty of confidentiality
d) The processing is necessary to protect the individuals "vital interests" (i.e. dietary/allergy requirements for an event which could lead to loss of life if not processed).

3.2 Principle 2: Obtaining and processing data for specified and lawful purposes only

3.2.1 Determine why we are collecting personal data and what we intend to do with it (our purposes)

Data controllers must be clear on why they are collecting an individual's data and what they intend to do with it and must inform individuals of these purposes.

As directed in the Information Commissioner's Office (ICO), it is important to be aware of the impact of the Privacy and Electronic Communications Regulations (PECR) on how you contact individuals. If an individual's data is collected as part of one individual type, they must give consent prior to individual data being used as part of another individual type (i.e. Individuals data being collected from a helpline call [1] but then being used to see if they wish to attend an event [2]). This can be achieved through a privacy notice (as detailed below in 3.2.2).

The PECRs also contain rules about direct marketing, which the ICO defines broadly to include "a wide range of activities that apply not just to the offer for sale of goods or services, but also to the promotion of an organisation's aims and ideals".

This means that newsletters or other calls to action (regardless of whether it contains a financial ask) could be interpreted as marketing material. If email addresses are used to send people information (such as newsletters) which could be construed as marketing material, you will need to specify this

purpose in your privacy notice (as detailed below in 3.2.2) and obtain consent from the individuals you intend to contact in this way.

3.2.2 Ensure data controllers give clear and accurate privacy notices to individuals when collecting their personal data

In our privacy notice, Allergy UK should include:

a) Who a staff member is/Allergy UK is
b) The purpose for which Allergy UK will process an individual's information
c) A consent statement if you intend to send the individuals marketing materials by email (including SmartMail) or text
d) Anything else you need to include to ensure there is nothing the individual would not expect.

If data is taken, this must be made clear verbally to the individual (if for a helpline caller) as well as on printed or electronic material (emails, website etc.). Otherwise the individual's data can only be used for the purpose whereby the individual gave consent. Consent must be "freely given, specific, informed and explicit". Therefore, silence (non-replies), pre-ticked 'opt-in' boxes or inactivity will not constitute consent and MUST NOT be relied on.

3.2.3 Notify the Information Commissioner

Allergy UK is registered on the Data Protection Register with the ICO. The data controller is registered as Allergy UK meaning that all Allergy UK staff have a duty to follow Data Protection rules.

A copy of the ICO document can be requested.

3.3 Principle 3: Ensuring data is adequate, relevant and not excessive:

3.3.1 Establish whether the information is relevant

All individual's data held by data controllers must be relevant to the purpose for which it was collected. Any data that is not relevant or will not be used must be deleted in accordance with Principle 5 unless:

a) There is a plan in place to use this data in the near future

And

b) Consent was given for this data to be held.

If the data collected is deemed excessive and is more than required for specific purposes, then it should be deleted.

3.4 Principle 4: Ensuring data is accurate and up-to-date

3.4.1 Ensure data held is not out-of-date to prevent prejudice of incorrect individual's data being processed

Data controllers must ensure that the following is adhered to:

a) Be able to demonstrate that you have taken reasonable steps to ensure the accuracy of any individual's data you obtain

b) Record the sources of individual's data you receive
c) Ensure challenges to the accuracy of individual's data are given proper consideration
d) Ensure the processes for updating individuals data are in place and that there is a follow up to any individual making a request
e) Ensure adequate safeguards are in place to prevent malicious alterations of personal information by those inside and outside of Allergy UK as detailed in Principle 6.

3.5 Principle 5: Retaining data

3.5.1 Ensuring that information which is no longer in use is destroyed as soon as possible:

Although no retention period is in place, data controllers should be able to justify the retaining of individuals data based upon the purpose for which it was collected. Data controllers must ensure that the following is adhered to:

a) Ensure personal data is deleted as soon as it becomes surplus to requirements. This includes electronic and paper copies, as well as any information held on database programmes. If a request was made by an individual then all data controllers must be aware and ensure data is deleted, unless consent was given by the individual for a separate data controller (on a different department or team) to hold this data for other purposes
b) Anonymise personal data when you no longer need to know who it relates to
c) Securely archive personal data such as case files which are no longer in use but must be kept
d) Ensure that data subjects know what will happen to their data when they have asked for it to be deleted, especially if individual's data is held across different departments or teams.

3.6 Principle 6: Information security

3.6.1 Ensure data controllers establish measures which will prevent harm to the individual as a result of their information falling into the wrong hands:

Although general I.T. and email systems are controlled by 3rd Party I.T. support, data controllers must ensure, as appropriate, that the following conditions are met:

a) Know who is in the building i.e. visitors, volunteers, cleaners, service users and ensure that physical records, IT equipment and building are secure. Every visitor to the office must sign in on arrival and sign out upon leaving.
b) Access to Allergy UK's network (including Wi-Fi) must only be given with the authorisation of 3rd Party IT support and the Chief Executive.
c) Data controllers should ensure that any personal data kept as hard copy (files, documents etc.) is secure.
d) Establish password procedures such as automatically expiring passwords. Staff as a whole are instructed to change their passwords every 45 days and must have a strong password in accordance with Microsoft standards. This is detailed in the I.T. policy.
e) Any individual's data kept on an electronic format (spreadsheets etc.) must be password protected.
f) Any individual's data kept on database programmes must require a data controller password to access.

g) Encrypt data when it is in transit, including on portable devices. Any individual's data that is to be transported away from the office, must be held on an encrypted device. This includes laptops and tablets. A USB encrypted memory stick is available from the Communications Team.
h) Monitor security logs showing failed attempts to log-in to your network. This is closely monitored by 3rd Party IT support. They receive alerts for any failed log-ins on the network and will advise Allergy UK of anything suspicious. If data controllers are concerned their workstation has been tampered with, they must report to the 3rd Party IT support.
i) Ensure ex-staff user accounts are disabled and passwords are changed for externally accessible systems. This procedure is currently in place by 3rd Party IT support. They need to be made aware if staff leave so this can be actioned.
j) Have a policy for home and remote working. This is detailed in the I.T. policy. As a guide, all home and remote working must require a password to access Allergy UK's network.
k) Ensure staff have been trained in their responsibilities under the GDPR. This is detailed in the Employee Handbook. All staff, whether data controllers or not, must also read this document as proof of compliance.

As well as the above criteria, staff as a whole must take steps to ensure information security:

a) Never disclosing passwords to anyone not connected to Allergy UK. If disclosed in error, the password should immediately be changed and 3rd Party IT support made aware.
b) If individual's data is kept in an electronic format and more than one staff member has the password to access it, then a log must be kept of who has the password to this particular data.
c) Workstations should always be locked (CTRL-ALT-DEL) when staff are away from their desks.
d) Any hard copy data that is needed for work, must be made secure once that work is completed.

4. General Principles

4.1 Rights of individuals

4.1.1 Ensure that data controllers are clear on the rights of individuals when dealing with their data:

a) right of access to a copy of the information that you hold about them
b) right to prevent processing for direct marketing
c) right to object to processing that is likely to cause or is causing damage or distress
d) right to object to decisions being taken by automated means
e) right in certain circumstances to have inaccurate personal data rectified, blocked, erased or destroyed
f) right to complain
g) right to data portability (in the case of digital images they supply to Allergy UK).

4.2 Understand individuals' rights for direct marketing

Direct marketing does not just refer to selling products or services to individuals, but also includes promotional activities of Allergy UK (such as newsletters). If an individual has signed up for a particular service by Allergy UK, it shouldn't be seen as giving consent for another service Allergy UK provides (e.g. Individual signing up for Allergy Alerts but then being placed on the Focus mailing list without prior consent), as detailed in Principle 2.

The Privacy and Electronic Communications Regulations (PECR) distinguish between individual subscribers and corporate subscribers with the effect that there are fewer restrictions on sending marketing materials to corporate subscribers. However, a "work email address" might still constitute as personal data. Therefore, it is good practice to gain prior consent before sending them direct marketing.

Prior consent can be attained via an "opting-in" to receive communications. The most important consideration should be to ensure the individual knows what they are signing up to.

4.3 Transfer of data abroad (outside the EU)

4.3.1 Ensure that all individuals' data is kept safe when travelling abroad:

Transfer of personal data to countries in the EU is permitted by the GDPR.

GDPR prohibits the transfer of personal data outside of the EU unless it is possible to ensure it will be adequately protected. Countries approved as having adequate safeguards include:

- Andorra
- Argentina
- Australia
- Canada (in some circumstances)
- Faroe Islands
- Guernsey
- Isle of Man
- Jersey
- State of Israel
- Switzerland
- USA (in some circumstances)

As a guide, consent should be given when travelling with individuals' data, even if from locations mentioned above.

5. Contacting us

If a person would like us to contact us in relation to this Data Protection Policy and our processing of personal information, then please contact us via email on info@allergyuk.org or by post at: Data Protection, Allergy UK, Planwell House, LEFA Business Park, Edgington Way, Sidcup, Kent, DA15 5BH.