ADVICE NOTE 5: APPGs AND DATA PROTECTION

Introduction

The Chair and Registered Contact of each APPG is responsible for the group's compliance with the law and the rules of the House.

This data protection audit is designed to help you to identify the actions needed to make sure your group complies with the Data Protection Act 1998 and the General Data Protection Regulation 2018. Attached is a template for the audit, with notes to help you. You will need to refer to the website of the Information Commissioner's Office.

Each APPG is different, and if your APPG holds or uses personal data in ways not outlined here, you may need to consult the Information Commissioner's helpline (0303 123 1113). In future your APPG may need to repeat the audit, and perhaps to take fresh action if it collects new types of data, uses data in a new way, or contracts with a new data processor.

This audit template is for guidance only. Parliamentary staff are not able to advise individual APPGs on data protection, or on the law. If you need more information please consult the website of the Information Commissioner.

The audit has three stages:

Stage 1: (Q1 and Q2): List the personal data which your APPG handles;

Stage 2: (Q3 to Q10): Work out how far your APPG meets requirements and what further actions are needed;

Stage 3: Plan, commission and undertake those actions.

APPG DATA PROTECTION AUDIT

Name of APPG:	
Date(s) of audit:	
Target date for completing actions: *(add this date after Stage 3)*	
Date actions were completed:	
Signature of Chair and Registered Contact:	
Signature of person undertaking audit:	

STAGE 1

LIST THE PERSONAL DATA WHICH YOUR APPG HANDLES

There are two questions to answer:

- What personal data does your APPG process?
  and
- Do any of these types of personal data include any special category data, or data about criminal offences (or similar)?

Q1: What personal data does your APPG process?

Personal data is defined in the General Data Protection Regulation ("the GDPR") as: "any information relating to an identified or identifiable natural person ('data subject')."

Almost anything you do with data counts as *processing*. This includes collecting, recording, storing, using, analysing, combining, disclosing or deleting it.

Hint: The Guide to the Rules for APPGs requires groups to compile and keep membership lists (both internal and external) and minutes. All APPGs will therefore hold personal data in these documents.

List below, *in the left hand column*, the types of personal data which your APPG processes. Below are some examples to help you. (There may be others.)

- names, email addresses and contact details (All APPGs will collect these for membership or mailing lists.);
- lists of those who attended meetings, and perhaps their views, as recorded in minutes or elsewhere;
- information about the experiences, health or personal circumstances of APPG members or others;
- information about individuals which has been collected during research;
- information about APPG staff, or individual contractors, which is used for payroll or contract administration;
- information collected via cookies about users of your website.

Types of personal data held or used by the APPG (Q1):	*Special category data, or data about criminal offences or similar matters? YES/NO (see Q2)*

Q2: Do any of these types of personal data include any special category data?

Special category data is broadly similar to sensitive personal data under the 1998 Act, except that there are now separate rules for processing data about criminal matters. It includes information about an individual's:

- race;
- ethnic origin;
- politics;
- religion;
- trade union membership;
- genetics;
- biometrics (if used for ID purposes);
- health;
- sex life; or
- sexual orientation.

Complete *the right hand column* of the table above to show which types of data include special category data, or data about criminal offences or similar matters.

Now move on to Stage 2. For some of Stage 2 you will need to consider in detail each of the types of data you have listed for Q1. If there is not enough space in the boxes provided, continue on a blank sheet.

STAGE 2

WORK OUT HOW FAR YOUR APPG MEETS REQUIREMENTS AND WHAT FURTHER ACTIONS ARE NEEDED

Q3: What is the lawful basis for processing this information?

Processing personal data includes collecting, recording, storing, using, analysing, combining, disclosing or deleting it.

The APPG must have at least one valid lawful basis for processing each piece of personal data. There are six possible lawful bases for processing, including consent: see https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/.

Hints:
• Most APPGs will rely upon "*legitimate purposes*" or upon the subject's *consent* as the lawful basis for processing membership information. If your APPG conducts outreach, the lawful basis for this may be *an activity carried out in the public interest that supports or promotes democratic engagement.*[1] • If you rely on people's *consent* for processing their data, the consent must meet legal requirements (see Q6).

If an APPG processes special category data[2], it must also meet an *additional* condition for that processing; for an explanation see: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/special-category-data/. In relation to criminal offences, see https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/criminal-offence-data/.

Action: List the lawful basis for processing each type of data you listed in answer to Q1. Add the condition which you meet for any processing of special category data. *Type of data (as listed in Q1)*	*Lawful basis (or bases) for processing. State the additional basis for any processing of special category data, or criminal offence data.*

[1] Data Protection Act 2018.

[2] Special category data is broadly similar to sensitive personal data under the 1998 Act, except that there are now separate rules for processing data about criminal offences and similar matters.

Q4: Has the APPG issued a privacy notice in relation to the information which it processes?

The GDPR says that personal data has to be processed lawfully, fairly and transparently.

All APPGs must provide a privacy notice[3] (also called a privacy statement) in clear and plain language at the time when they collect personal data from members and others. https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-be-informed/.

This notice must explain clearly the purpose behind collecting and holding this data, how long it will be kept, who it will be shared with and how people can exercise their rights (see below). The APPG must keep this notice up to date, and must reissue it if its practices change.

Good practice tip:

We recommend that each APPG should

- include a privacy notice in initial emails to its internal and external members, and to those who have asked to be on its mailing list;
- review its membership lists (and any other mailing lists it keeps) as part of an audit at least every 3 years, and
- send updated privacy notices each year;
- publish the privacy notices on its website (if it has one).

Actions: List the privacy notices sent out by the APPG, to whom they were sent and the dates of issue. Attach the notices to this document.

Privacy notice sent out	*Who it was sent to*	*Date it was sent*

Make notes below if the APPG needs to issue or reissue any privacy notices.

[3] A sample privacy notice for APPG members is included at the end of this document. You can find another one on the parliamentary intranet, included with the advice to MPs on data protection: https://intranet.parliament.uk/information-management/data-protection-security/data-protection/gdpr-for-commons-members/. NB: If you use either of these notices you must adapt them to your APPG's circumstances.

Privacy notice needed	*Is this a reissue of an existing notice, or new notice?*

Q5. Does the APPG allow individuals to exercise their rights in relation to personal data?

The APPG must allow individuals to exercise their rights, for example to access their data, to withdraw consent, or to have data corrected. https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/

Hint: We recommend that APPG secretariats and staff are trained to recognise requests from people who want to exercise their rights, and to enable them to do this.

Action: For each type of data listed under Q1, list the measures taken to ensure that individuals can exercise their rights. (This might include sending emails telling people about their rights, adding information to privacy statements, posting information on the APPG website, or training APPG staff to recognise requests.)

Type of data (as listed in Q1):	*Measures taken to ensure that individuals can exercise their rights:*

If the APPG needs to arrange training or to take other actions (such as amending privacy notices) to ensure that individuals can exercise their rights please make a note below.

Type of data (as listed in Q1):	*Measures needed to ensure that individuals can exercise their rights:*

Q6: If the APPG obtains individuals' consent when it obtains, holds and uses their personal data, does this meet legal requirements?

An APPG must obtain individuals' consent, and be able to show evidence of that consent, for using personal data if:

- no other lawful basis applies. See https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/consent/; or
- it processes special category data. This consent must be explicit.

Hint:
We also *recommend* that your APPG obtains and records explicit consent if it:

- uses the data for "direct marketing" (which need not be commercial); that is, any form of unsolicited outreach or survey by electronic means, such as email, text or phone calls; or
- uses cookies on websites.

See https://ico.org.uk/for-organisations/guide-to-pecr/what-are-pecr/.

The APPG must ask for consent in clear and understandable terms.[4] It must say exactly what the APPG or any third party is going to do with the data. It must also explain how the individual can withdraw consent, and it must keep accurate, dated records of that consent.

Actions:

- Check the types of data which the APPG processes, as listed in Q1, and list below those for which you need individuals' consent;
- Check whether individuals have given their informed consent, and whether they have given separate consent for special category data;
- Review the record of any consents the group has already obtained to make sure they are complete, informed and up to date;
- Attach the records of consent to the audit document.

Type of data (as listed in Q1) for which consent is needed	*Are records of this consent available?*	*Is this consent informed, and does it meet all requirements?*

If the APPG needs to obtain consent from any data subjects, or if it needs to refresh consent already given, make a note of this now. Make a note of any information which needs to be provided to ensure that consents are fully informed.

[4] There is a sample form at the end of this document. You can also find one on the parliamentary intranet, alongside official advice to MPs on data protection: https://intranet.parliament.uk/information-management/data-protection-security/data-protection/gdpr-for-commons-members/. If you use either of these you will need to adapt them to your APPG's circumstances. Make sure that you explain how to withdraw consent, and keep good records.

Type of data (as listed in Q1) for which consent is needed	*Is new consent needed or does consent need to be refreshed?*	*Key information requirements to ensure that consent is informed*

Q7: How long does the APPG keep this data? How does it make sure that it is not kept for longer than necessary, and deleted when no longer required or no longer current?

The APPG Chair and Registered Contact must make sure that data is not kept for longer than is needed; see https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/principles/storage-limitation/

Hint:
The Guide to the Rules requires the Chair and Registered Contact of an APPG to keep minutes and lists of internal and external members for **five years**. In addition he/she may need to keep other information for longer, for example HR or payroll information, if required by HMRC.

APPGs and their secretariats must delete personal information (such as email addresses) when it is no longer current, or when it is no longer required.

If the APPG ceases to exist, the Chair must either keep the minutes, membership lists, and other information, as required by the House, and the statutory authorities, until 5 years have passed; or he/she must make arrangements for someone else to do this.

If an APPG ceases to exist, or its secretariat changes, the Chair and Registered contact must make sure that the last secretariat returns or securely destroys any personal data it holds on behalf of that group.

Actions:

- For each type of personal data listed under Q1, list how long the APPG keeps this;
- List the arrangements in place to ensure that the data is kept no longer than needed;
- List the arrangements in place to destroy both hard copy and electronic data securely and confidentially.

Type of data (as listed in Q1)	*How long is it kept for?*	*How does the APPG ensure it is kept no longer than needed?*	*What are the arrangements for confidential destruction of unwanted data?*

If the APPG needs to take action to ensure that data is kept for no longer than needed, and that unwanted data is destroyed confidentially, please make a note of those actions now.

Type of data (as listed in Q1)	*Measures needed to ensure that data is kept no longer than needed, and/or destroyed under confidential conditions.*

Q8: How does the APPG ensure the confidentiality, integrity and security of this data?

The APPG must process data in a way which preserves its confidentiality, integrity and security.

https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/principles/integrity-and-confidentiality-security/

Action: For each type of data listed in Q1, record how the APPG processes this information and particularly how it stores the data; and what measures it takes to ensure confidentiality, integrity and security. This might for example include storing paper records in locked cabinets; encrypting emails; training staff in keeping and sending information securely; regular updates of mailing and membership lists etc.

Type of data (as listed in Q1)	*How is the data processed and stored?*	*What measures are taken to ensure confidentiality, integrity and security?*

If the APPG needs to take action to ensure the confidentiality, integrity and security of personal data, please make a note below.

Type of data (as listed in Q1)	*Measures needed to ensure confidentiality, integrity and security*

Q9: Has the APPG concluded a written agreement with a data processor in relation to this information? If yes, give the name of the data processor and the date of the agreement and attach it to this sheet.

The APPG must have a written agreement with any person or organisation who processes personal data on behalf of the group, if they are not employed by the group or by its officers.[5] That person or organisation is a 'data processor'. See: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/contracts/

Hint:
Any person or organisation outside Parliament is likely to be a data processor if they do any of the following in a way which involves processing personal data:

- providing secretariat services;
- undertaking surveys or research for the APPG;
- hosting the APPG's web presence, particularly if this involves cookies.

The agreement[6] must

- say what services the data processor will provide and
- set out contractual terms and
- require the data processor:

a) to ensure the confidentiality, integrity and security of the data;
b) to return the data to the APPG under secure conditions (or else to delete it) if it is no longer required;
c) not to subcontract any processing or to send this personal data outside the EEA without the APPG's explicit permission;
d) to allow individuals to exercise their rights, including withdrawing their consent to the processing.
e) to obtain individuals' consent to the processing of their data, if the data processor provides web services, and these involve cookies.

Hint:
Some companies, eg survey companies, transfer data outside the EEA. We recommend that APPGs' contracts with data processors forbid this without explicit consent.

[5] Almost anything you do with data counts as *processing*. This includes collecting, recording, storing, using, analysing, combining, disclosing or deleting it.
[6] A sample agreement is included at the end of this document. You can add to this but you must not shorten it.

Actions:

- List below any agreements which the APPG has with data processors, and the dates of these agreements, and append them to this document;
- Review the agreements. These must require the data processor to observe the standards set out for the APPG and described in this audit, particularly those set out at (a) to (e) above. If these documents do not exist or do not meet these standards, you will need to conclude and record new agreement(s) with your data processor(s);
- Make arrangements to review data processor agreements at least mid-parliament, and sooner if the arrangements change. For example if the APPG gets a new secretariat, or begins new research, it will need to update this agreement or prepare a new one.

Agreements already concluded with data processors	*Dates of agreements*

If the APPG needs to conclude any agreements with data processors, please make a note now.

Arrangements with data processors that need to be set out in formal agreements	*Is this a new or replacement agreement?*

Q 10: Does the APPG need to notify (register with) the Information Commissioner's office?

All APPGs must follow the data protection principles and good practice.

Some APPGs will also need to notify (register with) the Information Commissioner's office. They will not need to do this if they are not for profit organisations processing data only for the purposes of establishing or maintaining membership or support for a not for profit body or association, or providing or administering activities for individuals who are members of that body or have regular contact with it.

Action: if needed, do the test on the ICO website (https://ico.org.uk/for-organisations/data-protection-fee/) to see if the APPG needs to register with the ICO (see Chapter 4 of the booklet at the link above). Make a note if you need to register.

STAGE 3

MAKING SURE THE APPG COMPLIES

In consultation with the Chair and Registered contact of the APPG, review the records you made at Stage 2, and the notes you made about actions needed. Make an action list, using the template on the next page. Set a target date for completing each action, and agree who will be responsible for it.

Depending on the circumstances, the actions needed might include:

- Issuing or replacing privacy notices (see Q4);[7] [8]
- Taking steps to ensure that people can exercise their rights in relation to their personal data (see Q5);
- Obtaining or refreshing individuals' consent to process their personal data (see Q6);[9]
- Taking steps to ensure that data is kept no longer than necessary, and that unwanted data is destroyed confidentially (see Q7);
- Taking steps to ensure the confidentiality, integrity and security of personal data (see Q8);
- Concluding or updating agreements with data processors (see Q9)[10];
- Notifying the Information Commissioner's office and paying a fee (see Q10).

Set a target date for completing the programme of actions.

Now commission those actions. Once everything is completed, don't forget to update the front page of this audit. Check that you have attached any necessary documents, such as the records of any consent given, any privacy notices issued, and any data processor agreements concluded. Keep these records securely.

---

[7] A sample privacy notice for APPG members is included at the end of this document. You can find another one on the parliamentary intranet, included with the advice to MPs on data protection: https://intranet.parliament.uk/information-management/data-protection-security/data-protection/gdpr-for-commons-members/. NB: If you use either of these notices you must adapt them to your APPG's circumstances.

[8] If the APPG collects, holds or uses other types of personal data, or uses personal data for purposes not included in the privacy notice provided, it will need to take further action. For example the APPG will need a further privacy notice if it collects personal data for the purposes of research, or from its website.

[9] There is a sample form at the end of this document. You can also find one on the parliamentary intranet, alongside official advice to MPs on data protection: https://intranet.parliament.uk/information-management/data-protection-security/data-protection/gdpr-for-commons-members/. If you use either of these you will need to adapt them to your APPG's circumstances. Make sure that you explain how to withdraw consent, and keep good records.

[10] A sample agreement is included at the end of this document. You can add to this but you must not shorten it.

LIST OF ACTIONS TO BE TAKEN FOLLOWING APPG DATA PROTECTION AUDIT

Action needed	*Person to be responsible*	*Target date for completing the action*

SAMPLE DATA PROTECTION PRIVACY NOTICE FOR AN APPG

To adapt and publish/send out to those on membership and mailing lists

---

The APPG on …….. processes your personal data for the purposes of maintaining and using a membership [or mailing] list, and keeping minutes of meetings.

The data controller is …… who can be contacted via ……

The data which we obtain from you and process is

- Your name, title and email address
- Your phone number
- Your role (eg MP for XXX), and/or the organisation that you work for (if any)
- *(if applicable)* your address

We use this information to send you information about the APPG and its work, including meeting notices and minutes. *If applicable:* We may also record personal information about you, including your opinions, in minutes of meetings.

Our lawful basis for using this information is *[set out here your chosen one or more of the 6 lawful bases]*

We will hold this information securely and we will keep this information for five years.

Either

- we will not transfer this personal data to any other organisation

or (if applicable)

- we will share this personal data only with our contracted data processor(s), who is/are…….. This organisation is contracted to provide membership administration/a secretariat for the APPG.

Please also note that under the rules which Parliament has set for APPGs, the names of APPG members (but not their contact details) are published on the group's website or webpages (if it has one) or else provided to enquirers on request.

If you have questions about the use of your personal data or you wish to amend or correct it, you should contact the APPG'S Chair and Registered Contact whose details you can find from the APPG Register https://www.parliament.uk/mps-lords-and-offices/standards-and-financial-interests/parliamentary-commissioner-for-standards/registers-of-interests/register-of-all-party-party-parliamentary-groups/ or (in the first instance, if applicable) the Secretariat.

Date of notice ……

SAMPLE DATA PROTECTION CONSENT FORM FOR AN APPG

To adapt and send to individuals in relation to the processing of personal data (eg for membership administration)

This form could be used to obtain individuals' consent for the processing of data necessary for maintaining a mailing and/or membership list and keeping minutes. To use it for other purposes the form would need to be adapted.

I [name]…….

[email address] ……consent to the APPG on……. ……...using my name and contact details only for the purposes of maintaining a membership list and keeping minutes.

I give my consent on the understanding that

- my name will be included in the APPG's membership lists, and that these are kept for five years;
- my name and contact details will not be shared with any third party except…….. ……[if it will be shared with a secretariat or other person or organisation outside Parliament, who will be data processor for the APPG, please explain who this is and what will happen to the data];
- lists of members and of roles or job titles (but without contact details), and minutes, will be posted online on the APPG's website, or (if the group has no website) made available on request, as required by the rules of the House;
- the APPG (or its contracted data processor (if named above)) will contact me about meetings and other developments and these contacts will/will not include proactive emails about relevant developments or other matters;
- The APPG, and its contracted data processor (if named above) will process my personal data securely. The APPG will not allow this data to be shared with any other subcontractor or sent outside the EEA without its explicit permission.

Signed…….

Date……

You have rights in relation to this data. You can exercise these at any time. For example you can ask to see what data is held about you, or to withdraw your consent. To exercise these rights, email or write to the Chair and Registered Contact. You can find their details from the

Register of APPGs: https://www.parliament.uk/mps-lords-and-offices/standards-and-financial-interests/parliamentary-commissioner-for-standards/registers-of-interests/register-of-all-party-party-parliamentary-groups/.

SAMPLE DATA PROCESSOR AGREEMENT FOR AN APPG TO ADAPT AND CONCLUDE WITH ITS EXTERNAL SECRETARIAT

This agreement is between [……..], who is the Chair and Registered Contact of the APPG on [……..] (the "Data Controller"), and …… (the " Data Processor"). It is effective from [……to……].

The purpose of this Agreement is to ensure that the arrangements for processing personal data on behalf of this APPG comply the requirements of the House and with the law, in particular with obligations under Regulation (EU) 2016/679 of the European Parliament and of the European Council, as supplemented by the Data Protection Act 2018.

The Chair and Registered Contact of the APPG is the **data controller** for this personal data. The **Data Processor** agrees to process the data only in accordance with Data Protection Act 2018, the General Data Protection Regulation and the Privacy and Electronic Communication Regulations.

1. In particular, the Processor will process this data only

- in accordance with written instructions from the APPG chair or nominated representative;
- having implemented sufficient technical and organizational measures to ensure its confidentiality, integrity and security. This includes placing staff under a duty of confidence.

2. The Processor will

- report data breaches to the Controller and/or the ICO without delay (see https://ico.org.uk/for-organisations/report-a-breach/);
- cooperate with the Controller and relevant authorities if a data access request is received or if there is an inquiry by the Parliamentary Commissioner for Standards, auditors or others.

3. The Processor will not

- use this personal data for its own purposes, such as its own campaigns or sales;
- use subcontractors, or send the personal data outside the EEA (unless specifically agreed in writing with the Data Controller);
- keep the data beyond the retention periods agreed with the APPG Chair and Registered Contact.

4. This agreement will end at the date set out at the top of this page, or earlier in any of the following circumstances

- after a month's notice is given by either party, or
- at the end of the fourth day after a General Election, if the MP loses his/her seat or does not stand again;
- one month after the data controller ceases to be an MP at any time other than at a General Election (beginning with the date on which he/she ceased to be an MP).

5. When this agreement comes to an end the data processor will transfer the personal data to the data controller (or, if deceased, to their personal representatives) no later than one month after the end date of the agreement, as set out in the paragraph above.

Chair and Registered Contact……

Name of APPG…….

Name of data processor……..

Name of data processor's data protection officer……

Date of signing……

Document owner: Registrar of Members' Financial Interests
Date of document: 5 September 2018. Updated 11 December 2019.
For advice contact: groupsregister@parliament.uk or 020 7219 0401