APCC Privacy Statement on GDPR – APCC Business related activities

Introduction

1. The General Data Protection Regulations (GDPR) come into force on 25 May 2018, and bring into force new rules about how organisations can handle personal data.
2. This statement sets out what personal data the APCC holds, our business purposes for processing that data, the lawful basis we have for doing so, who we share that information with, your individual rights in relation to that data, and some ancillary information about data security, data retention (how long we hold the data) and data breaches.
3. This document is intended to serve as a 'privacy statement' within the requirements of the GDPR to explain how we handle personal data for APCC Business related activities.
4. Please note that we have developed a separate **APCC Privacy Statement on GDPR for Internal - HR** which is made available to all employees.

Business Purpose for Processing Data

5. We have four key business purposes for processing personal data:
   I. The effective **personnel management** i.e. APCC staff and contractors as well as recruitment functions. Note that this is contained in a separate Employee Privacy Notice and so is not considered further in this privacy statement.
   II. To contact **our members** (Police and Crime Commissioners and equivalents and their staff), consult and gain their views on relevant issues, and enable them to contribute to the development of national policy and related initiatives in the policing and criminal justice landscape.
   III. To engage with our **partner organisations**, so that our members can influence national policy on policing, criminal justice and related matters. Our partner organisations include other organisations with a role in developing law, policy, guidance or practice impacting on the role of our members. An indicative list of these organisations is set out at Annex A for information.
   IV. To assist **members of the public** who have contacted us for help or advice about specific issues.

The 'Business Related' personal data we hold

Our members

6. In relation to Police and Crime Commissioners, their equivalents and staff ('our members'):
   - For those members that are APCC Board members, we hold details of names, home and email addresses, dates of birth and telephone numbers as required for registering at Companies House as Directors.
   - For all our members, we hold business email addresses, postal addresses and telephone numbers. We may also hold home and personal email addresses and phone numbers, where members have supplied these to us to better facilitate communication.
   - We hold "special category" data in relation to our PCC and Mayoral members as set out below.

Partner Organisations

7. We hold business email and postal addresses, and business telephone numbers. **Annex A** (below) sets out an indicative list of our stakeholders / partner organisations.

Members of the public

8. We hold information they have supplied to us, to enable us to respond to them. This may include home or business addresses, personal and/or business email addresses and personal or business phone numbers. This may include some "Special Category" data – but only where the member of the public has offered this information to us of their own volition.

Lawful Basis for Processing Personal Data

9. The GDPR sets out 6 possible lawful bases on which organisations might process data, depending on their functions and legal status. As a membership organisation for Police and Crime Commissioners (and other similar bodies) and their offices, we only handle a limited amount of personal data (see previous section), but do need to be able to process that limited amount in order to effectively fulfil the business purposes set out above.
10. We have therefore determined that our lawful basis for processing personal data is that of "legitimate interest".
11. We understand that this basis places obligations upon us to use people's data in a way they would reasonably expect, and that we are taking on responsibility for considering and protecting people's rights and interests and balancing this against other legitimate interests, such as that of third parties and wider benefits to society.

"Special Category" Personal Data

12. The GDPR contains specific requirements about the handling of "Special Category Data". This is personal data which is regarded as particularly sensitive and includes race, ethnic origin, politics, religion, health, sexual orientation, genetic information, etc.
13. In order to process special category information, organisations must satisfy a specific condition (from a limited range set out in Article 9(2) of the GDPR). The following applies:

    - **Our members** - Given that our members are elected politicians, we hold information about the political party they belong to (which counts as 'special category' data), in order to help us gather their views and influence national policy.

      The specific condition under which we process this special category information, is Article 9(2)(d) i.e. that this is carried out (with appropriate safeguards) as part of our legitimate activities as a not for profit member association.

    - **The public** – The information provided to us by members of the public may include some "Special Category" data – but only where the member of the public has offered this information to us of their own volition.

Sharing Personal Information

14. Our Members' Personal Data – Where we hold personal data, we do not generally share this without the permission of our member, except in exceptional circumstances i.e. a critical incident where it is urgent a third party is able to contact a member
15. Personal data belonging to members of partner organisations – Where we hold personal data, we do not generally share this without the permission of the data subject, except in exceptional circumstances i.e. there is an urgent need that a third party is able to contact that person.

16. Personal information from members of the public – unless there is a compelling public interest in doing so (i.e. to protect your safety or that of other people), we do not share this data without first seeking the agreement of the member of the public (for instance, if it is a complaint or problem raised about the local police force, we will ask your permission to share your contact details with the local PCC, so the matter can be resolved).

17. We will not transfer personal data to countries outside the EEA.

Your Rights

18. The GDPR protects the rights of individuals about how personal information is held. Individuals have the following rights (except in certain specific circumstances):

    1. *The right to be informed about the collection and use of your personal data* - This means we must explain our purposes for processing your personal data, our retention periods for that personal data, and who it will be shared with. That is what this document aims to do.

    2. *The right of access* – this allows you the right to be aware of the personal data and any supplementary information we hold about you and allows you to check that our processing is lawful. However, we must verify your identity before allowing you access.

    3. *The right to rectification* – you have the right to ask us to correct your personal data where it is inaccurate or incomplete. You can make this request either verbally or in writing and we must respond within one month. We do not have to make a change if we think the data is accurate or if we believe the request is manifestly unfounded or excessive.

    4. *The right to erasure* – you can ask us to erase your personal data (also known as the 'right to be forgotten'). The section below on Our Data Protection Policy sets out information about how long we would normally retain data before erasing it, but if you want us to erase personal data before the end of that period, you can ask us to do so, either in writing or verbally. We will respond within one month, and we can only refuse to erase personal data in a limited number of circumstances which are set out in the ICO guidance (https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-erasure/)

    5. *The right to restrict processing* – you can ask us not to share your personal data (as set out in the section on Sharing Personal Information), if you have contested the accuracy of the data or our lawful basis for processing it, during the period when we are considering your request. You can also ask us to hold your data but not share it, where we would normally delete under our retention policy, but you need us to keep it in order to establish, exercise or defend a legal claim.

    6. *The right to data portability* – this right only applies where the lawful basis for processing is consent or for the carrying out of a contract, and processing is carried out by automated means. These conditions do not apply to the APCC or the personal data we hold.

    7. *The right to object* – you have the right to object to our processing your personal data based on legitimate interest, (which is the lawful basis we use for processing personal data). We must comply with your request unless we can demonstrate compelling legitimate grounds for the processing, which override your interests, rights and freedoms. These circumstances would have to be exceptional.

    8. *Rights in relation to automated decision making and profiling* – the APCC does not use these.

Our Data Protection Policy

19. Out Data Protection Policy deals in more detail with the measures we take to protect your data. Our full policy can be found in our **APCC Internal Data Security Policy Statement: APCC Business** [link].

20. However, we have set out below a summary of the key information you should be aware of.

    1. **Data Retention Policy –** this sets out a summary about how long we retain different types of personal data before we delete it. This varies according to the type of personal data it is:

        - **Unsuccessful Job Applicants** – we hold personal data for 6 months for individuals that have applied for jobs with the APCC but do not become employees.
        - **Police and Crime Commissioners, their equivalents and staff** – Where we hold personal data on these individuals, we retain it only as long as they are in office/post and for a period of 6 months after they have left office unless we are asked to destroy it earlier or are asked to retain it longer by the data subject.
        - **Partner Organisations** – we retain personal details until we are informed that the individual concerned has left their post in that organisation.
        - **Members of the Public** – We will retain members of the public personal data for 6 months from the date you contact us, or six months from the date we last provided advice or help to resolve your issue, where appropriate, unless we are asked to destroy it earlier or are asked to retain it longer by the data subject.

    2. **Information audit** – We have undertaken an internal audit to identify the types of personal information we hold. This is set out in 'The 'Business Related" Personal Data We Hold' section of this policy.

    3. **Security measures** – The APCC takes the security of business-related personal data seriously. We have controls in place to protect personal data against loss, accidental destruction, misuse or disclosure and to ensure that data is not accessed, except by employees in the proper performance of their duties. The APCC:

        - Keeps paper-based personnel files kept in locked drawers.
        - Maintains a "cloud" based HR Database which is located in a UK web hosting data centre that is physically secure with servers protected by industry standard Windows firewalls, with advanced monitoring and blocking tools to protect against any attempt at unauthorised system access. Key employee information is encrypted in the database, ensuring that only individuals with requisite access permissions can access data and process data.
        - Will provide training to all individuals about their data protection responsibilities as part of the induction process and at regular intervals thereafter.
        - Will ensure that all email signatures contain references to our GDPR Policy as well as making this available on our website.
        - Will ensure that all applicants for APCC Jobs are advised of our data retention policy as part of our application pack.
        - Uses Loop Management Services for the destruction of hard copy sensitive information.

        APCC Employees who have access to personal data are required:

        - To access only data that they have authority to access and only for authorised purposes.
        - Not to disclose data except to individuals (whether inside or outside the APCC) who have appropriate authorisation.

- To keep data secure (for example by complying with rules on access to premises, computer access, including password protection and secure file storage and destruction).
- Not to remove personal data, or devices containing or that can be used to access personal data, from the Company's premises without adopting appropriate security measures (such as encryption or password protection) to secure the data and the device.
- Not to store personal data on local drives or on personal devices that are used for work purposes.
- To take care to ensure that PC screens and terminals are not visible except to authorised APCC employees.
- To take care that manual records:
    - Are not left where they can be accessed by unauthorised personnel and may not be removed from business premises without explicit written authorisation.
    - Are destroyed using secure methods as soon as they are no longer required.
- To report data breaches of which they become aware to Oliver Shaw immediately.

4. **How we report data breaches** - A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. If a breach does occur, we must inform the Information Commissioner within 72 hours. We must also notify you as soon as possible if the breach carries a high risk to your rights and freedoms. In the unlikely event that this occurs, we will discuss with you how best to address any adverse consequences that might arise from the breach.

5. **Our Data Protection Officer** – Although we are not required to appoint a Data Protection Officer, we have decided to do so, to help monitoring our compliance with the GDPR and other data protection laws, our data protection policies, awareness-raising, training, and audits. If you have any concerns about your data or how we process it, you should contact the DPO in the first instance using the details set out below (under Contact, Complaints and Concerns).

Contact, Complaints or Concerns

21. If you have concerns or queries about how we handle your data, you should contact our Data Protection Officer: Oliver Shaw, Director Policy and Strategy.
22. If you are not satisfied with how we have handled your query or the action we have taken as a result, you can:
    - Contact the APCC Chief Executive at dawn.osborne@apccs.police.uk
    - Contact the Information Commissioner (see their website - https://ico.org.uk/)
23. In some circumstances, you might also be able to enforce your rights through legal action/the courts. You may want to seek independent legal advice about this, where appropriate.

Annex A

Indicative List of our National Partner Organisations

The following is an indicative list of the main national partner organisations where we hold the business email and postal addresses and business telephone number of some staff and officers:

- Government Departments, particularly the Home Office and Ministry of Justice
- Her Majesty's Inspectorate of Constabulary and Fire and Rescue Service
- The College of Policing
- Independent Office of Police Conduct
- National Police Chiefs Council
- National Fire Chiefs Council
- National Crime Agency
- Members of Parliament
- National Media Organisations
- Police ICT Company
- Unions and Staff organisation representing members in the criminal justice sector
- Large National Level Voluntary Organisations, such as Independent Custody Visitors Association, Victim Support, Neighbourhood Watch, Women's Aid, linked to the criminal justice sector
- Information Commissioner's Office