The Data Protection Act 2018 (DPA) and the General Data Protection Regulation (UK) 2016/679 (GDPR) compliance policy and guidance

Introduction

A guide relating to UK Data Protection Act 2018 (DPA) and the UK General Data Protection Regulation (UK GDPR) compliance that details the corporate responsibility owed by all staff to the Commissioner of Police of the Metropolis, [*as designated Met Data Controller*] to ensure full compliance with the provisions of the DPA.

The GDPR superseded the Data Protection Directive 1995 and all member state law based on it on 25 May, 2018. The DPA came into force at the same time, modifying the GDPR by filling in sections that were left to individual member states to interpret and implement. The DPA 2018 also applies “a broadly equivalent regime” – which it calls “the applied GDPR” – to certain types of personal data processing that fall outside the EU GDPR’s scope, including processing by public authorities. It also sets out data processing regimes for law enforcement and intelligence purposes. The DPA 2018 supports the GDPR rather than enacting it, the two laws should be read together.

The GDPR is retained in domestic law as the UK GDPR.

The data protection law applies to any processing carried out by the Metropolitan Police Service (Met) and its staff whereby personal or special category personal data of any living person (known as a “data subject”) is collected, recorded, or otherwise processed.

Furthermore, the guide directs Met personnel to always seek specialist DPA advice directly from the Data Office and to ensure they refer all internal and external data protection enquiries, requests and applications to the Data Office promptly in line within any statutory time periods.

Information Management

Data protection - main responsibilities

Every day the MPS processes a large amount of personal data or special category personal data for various policing purposes; so you need to be aware what you have to do to ensure it is always recorded and processed correctly and handled securely in accordance with your policing role and duties.

All MPS staff, individuals who form MPS Sub Groups, and individuals who handle and/or process any personal data, or special category personal data on behalf of the MPS, are required to have adequate knowledge of the DPA in order to adequately protect personal and special category personal data in line with the MPS’ legislative

and regulative obligations. You must ensure you are familiar with these and that you have:

- Read, digested and put into practice all data protection requirements documented within this guide. Besides identifying what constitutes personal data, you will also need to have adequate knowledge of the DPA 2018 and its six data protection principles (and other requirements) to ensure legal compliance. It is to be noted that most of the information the MPS process is information collected and held for policing purposes and the processing of this information is regulated by Part 3 of the DPA 2018 which deals with law enforcement, while instead personnel information which falls under HR, OH, Pay and Pension and all other information collected, held and processed for non-policing purposes is regulated by the UK GDPR and by Part 2 of the DPA 2018
- Checked whether your local data processing is satisfactory. Re-assess how the personal data you handle is recorded/ processed in order to ensure it is properly protected.
- Considered what good practice and data handling rules are appropriate to protect personal data and special category personal data from the potential threat of its loss or compromise.
- Understood any requirements to move personal data, particularly sharing or disclosure externally, which must only be undertaken in a legal, secure and accountable manner. If your duties involve the lawful sharing or disclosure of personal data outside of the police service, ensure that you have the right legal authority to make such decisions; that such decisions are properly recorded for an audit trail and that any personal data is exchanged with third parties in a secure manner.
- Followed DPA processes by ensuring you have sought expert advice or referred matters directly to the Data Office, especially in cases where a statutory time period applies. If you have any data protection query or are not sure how to deal with any personal data always contact the Data Office first. Do not contact the Information Commissioner's Office (ICO) or the Directorate of Legal Services (DLS) directly for advice on specific issues as the Data Office will liaise with those bodies on behalf of the data controller should such action be required.

Definitions

Definition the DPA 2018 (the DPA) is designed to set conditions in order to protect personal data/special category data that relate to identifiable living persons known as data subjects.

Personal data only includes information relating to natural persons who:
- can be identified or who are identifiable, directly from the information in question; or
- who can be indirectly identified from that information in combination with other information.

Personal data may also include special categories of personal data or criminal conviction and offences data.

These are considered to be more sensitive and may only be processed in more limited circumstances.

Scope The DPA controls how personal information is used by organisations, businesses or the government.
The DPA covers all personal data, held in any format, on computer systems or in any other formats, such as paper records, photographs, CCTV and more.

DPA Training

How to enrich your data protection knowledge – Mandatory Training

The Information & You course has always been mandatory since its launch in May 2018. It replaced the former Computers and You, which was also compulsory.
The Acceptable Use Policy which states that new Foundation account holders must complete it or their accounts may soon be disabled [redacted].

If you have not completed the course yet please do so now. The course can be accessed by following the below link:

[redacted]

Six Data Protection Principles

The role of the data controller (which at any time may be MPS) is to ensure that anyone processing personal data under their direction [*i.e. the data processors*] must comply with six key data protection principles of good practice which require that personal data and/or special category personal data is [*always*] dealt with as follows:

- DPA Principle 1 - Processing must be lawful and fair;
- DPA Principle 2 - Purposes of processing must be specified, explicit and legitimate;
- DPA Principle 3 – Personal data must be adequate, relevant and not excessive in relation to the purpose for which it is processed.
- DPA Principle 4 – Personal data must be kept accurate and up to date;
- DPA Principle 5 – Personal data must be kept no longer than is necessary; and
- DPA Principle 6 – Personal data must be processed in a secure manner.

Under the UK GDPR and the DPA, a processor also has a responsibility to challenge processing and methods of collection.

Data Security

Personal data demands protection – note on DPA Principle6

Under the DPA, you should protect everyone's personal data with the same degree of care you apply [or would expect to be applied] to your own personal data/special category personal data.

All data subjects are entitled to expect a consistent and high standard of protection to be applied under the DPA [*see DPA Principle 6*] for any personal data that relates to them and which is being held by the MPS. This security requirement applies whether or not data subjects are otherwise identified/ classified [*by the MPS or in legislation e.g. PACE*], for example, as a victim, witness, arrestee/ suspect, informant, member of staff; all of which are factors that are immaterial in this context. In this respect the DPA is neutral as regards the status, gender or any other characteristics of data subjects and this protection for personal data/ special category personal data must always be applied equally both on an individual or collective basis. It also means that the MPS must at all times adequately protect any personal information from unauthorised disclosure.

You also need to be aware that data subjects are also granted a number of specific rights under the DPA:

- Right of access
- Right to be informed
- Right to rectification
- Right to erasure and Right to restriction
- Right not to be subject to automated decision-making

The Data Office handle all of the above requests.

Please note - you will have already noticed that the DPA 2018 only applies formally to living individuals and the Data Rights Unit will deal with requests for information submitted by living individuals.

So if you ever receive a request for information about a deceased person in relation to specific incidents and the deceased individuals' involvement, from their family or legal representative, you should refer the request to the BCU/OCU or to the officer who investigated the matter.

They will need to request the following:

- Proof of death
- Proof of ID of the requester
- Proof of relationship with the deceased
- Proof of address

An appropriately ranked decision maker will need to carry out a risk assessment in order to identify any potential risks in disclosing the information. A decision and the rationale for the decision should be added on to CRIS. For further advice on this type of requests for information you can contact a Band C within the Data Rights Unit or DLS.

Requests may be received in the form of a Freedom of information Act 2000 (FoIA) request, but this may not be seen suitable legislation to meet the request as there may be an outstanding duty of confidence to the deceased individual or the release of information may breach the DPA or HRA rights of a third party. However, should you receive a request for information about deceased individuals, which makes reference to FoIA, you may wish to contact a Band C within the Data Rights Unit who can advise you on how best to deal with the request so not to breach the FoIA.

If the information requested relates to the service history or other employment data of a deceased former member of the MPS this should be referred to the MPS Historical Collection or Records Management Branch.

International data processing – note on DPA Principle 6

The general rule under DPA Principle 6 is that personal data/special category personal data is NOT to be transferred beyond UK borders; EXCEPT for the lawful transfer of personal data between countries within the European Economic Area (EEA) and with a small number of listed/ approved countries outside of Europe with comparable data protection legislation.

Please note the list of countries outside Europe can be subject to change and additionally a number of international agreements are no longer valid. You should therefore appreciate that both the political climate and the law/ processes in the area of international data processing has become increasingly complex and fluid in recent years.

For example the former but limited data protection agreements between the USA and the EU, known as Safe Harbor and the EU-US Privacy Shield are no longer to be used due to a recent US presidential executive order revoking these agreements. Alternatively, some existing contracts may contain approved EU data processing agreement clauses [*terms and conditions*] and if so they will remain valid, but this does not set any precedent and cannot be extended beyond the contractual arrangements in question. The lawful transfer of personal data between EU countries and the USA will, although feasible in theory [particularly on international crime/national security grounds], due to the tricky legal issues involved, it means you should always check this aspect out well in advance by seeking expert advice. This will ensure that there always remains a sound basis for international personal data sharing/ or processing.

Always seek expert guidance in advance from the Data Office unless you are already following an established international data exchange process you are familiar with, [*such as under Schengen (European arrest warrants system) and the European Investigation Order (EIO)*].

If you receive any request to send personal data outside of the UK and it is not by using a previously approved service [*such as under Schengen or EIO*] contact a Senior Privacy Advisor within the Data Office by writing to MPSDataOffice@met.police.uk

Fair processing and consent for data processing

The data controller for the MPS is the Commissioner of Police of the Metropolis who is responsible under the DPA for determining what and how personal information will be processed. Day-to-day processing of personal data/special category personal data is undertaken by MPS personnel and data processors as described above. Privacy Notices (PNs) - the data controller is required to be transparent and specific in advance about how this personal data is to be used so that data subjects are made aware of the manner of data processing and can challenge it. This means issuing/displaying privacy notices making it clear how personal data will be processed and protected etc. in line with the purposes for which it was collected. The MPS Privacy Notice is published on the MPS website and lists the main policing purposes for collecting personal data. If you wish to access the MPS Privacy Notices you can do so by following the link below:
https://www.met.police.uk/search?q=privacy+notice

A child friendly version of the MPS Privacy Notice has recently been added and it can be showed or shared with children that you may be aware wish to know more about how we process data that we may need to collect from them.

Consent requirements - it is common under the DPA for data subjects to be asked to provide consent to allow any data processing. However, under the DPA - Schedule 2, Part 1, Paragraph 2(1) the prevention and detection of crime exemption allows the MPS to use personal data for a legitimate policing purpose without having to actively seek explicit consent from individuals.

For example, under PACE there is already a legal requirement upon someone under arrest to provide their name and address details. Seeking consent in such circumstances would not be appropriate or make any sense as it would frequently invite refusal by data subjects.

It should also be noted that even when the MPS shares or discloses personal data to third parties, it is often not necessary to seek consent from individual data subjects. The conditions to allow this to take place are when an overriding legal duty/power exists that allows sharing/ disclosure in principle and where the public interest in sharing/disclosing outweighs an individual's privacy rights under the Act. An obvious example might be where the police share personal data with other public agencies to safeguard a minor under child protection legislation.

But remember, if you are ever unsure as to whether or not consent should be required from data subjects, first of all seek advice directly from the Data Office.

Submitting Right of Access Requests (ROARs)

Right of Access Requests (ROARs) (Previously Subject Access Requests (SARs) under DPA 1998) allow individuals to find out what personal data organisations such as the MPS are holding about them. This is one of the main rights under the DPA. The Data Office – Data Rights Unit - currently processes approximately 7000 ROARs on behalf of the MPS each year.

If you believe an individual has made or wishes to make a ROAR but you are not sure what to do next, please contact the Data Rights Unit immediately for advice by email to MPSDataOffice@met.police.uk

The ROARs application process

Members of public should be directed to MPS website to submit a request for information – https://www.met.police.uk/rqo/request/ri/request-information/

Step 1 - Applicant's proof of identity and address

The applicant should send their completed application in together with proof of identity (ID). To confirm the applicant's identity the Data Office needs to see evidence of official document(s) that should provide sufficient information to prove their:

- Full name;
- Date of birth;
- Current address; and
- Signature.

Acceptable ID - The Data Office maintains a list of acceptable documentation, but typically this will include a combination of passport; driving licence; birth/ adoption certificate; medical card; bank statement or utility bill. If an individual is using a driving licence as proof of address, it must have been issued within the last 6 months. Photocopies of documents are usually acceptable; however the Data Office reserves the right to request original documentation in some cases.

Proof of address - if the applicant cannot provide full proof of address, as for instance, when staying with a friend or living in temporary accommodation, they should ask their friend or warden to write a letter to submit with their form. This letter should explain that they have permission to stay at that address and this should be on headed paper or officially stamped. Alternatively the applicant can provide a sworn affidavit. If the applicant is serving a term of imprisonment they must ask the prison governor to confirm this fact.

The cost of an application – The MPS no longer charges for processing ROARs.

Step 2 – Delivery of completed ROARs

Posted applications must be sent to MPS Data Rights Unit, PO Box 313, Sidcup, DA15 0HH

Courier delivery - if an applicant wishes to arrange for a courier firm to deliver their ROAR they should give their courier the following address: MPS Data Rights Unit, PO Box 313, Sidcup, DA15 0HH.

Advise the applicant that this address can only receive mail delivered by official courier, as delivery by anyone else will result in refusal. The courier would need to identify themselves at Reception and explain they have mail for the Data Rights Unit.

Step 3 – Consider ROARs submitted by someone other than the Data Subject

The general rule is that the ROAR process can only be used to apply for your own personal data.

Right of access is fundamentally a confidential process between the data subject and the data controller [i.e. the MPS Commissioner]. There is no general DPA provision for someone [*other than the data subject*] to submit a ROAR and so be able to receive someone else's personal data. Consequently such applications will be refused in accordance with the DPA.

Therefore, the DRU cannot provide an applicant [*who is not the 'data subject'*] with the details of another person under this provision ***unless*** the DRU is satisfied there is good reason why the data subject cannot apply themselves ***and*** they have also provided specific consent for release of their personal data to another person [*such as their solicitor*].

Besides being given relevant consent, the DRU may also ask to see proof that the third person applying on behalf of the data subject has sufficient status/ legal authority to act on behalf of the other person in this regard. This is because the practice of 'enforced right of access' under DPA is a criminal offence.

There are two valid and fairly common exceptions to this rule:
1) When a parent/guardian acts in the best interests of a young child [Parents can apply for information for children under the age of 13. From the age of 13 onwards children can apply independently] the responsible adult can apply on behalf of their child.
2) When a vulnerable adult is unable to provide valid consent [*e.g. due to mental or other incapacity*] another person acting lawfully in the data subject's interests can do so. This could include the person's next of kin/their care provider, with a power of attorney or a solicitor.

It is to be noted that After having located the information requested the caseworker may deny the third person access to the information they requested on behalf of the data subject in case they identified a risk of harm to the data subject as a consequence of the information being disclosed to the third party (i.e. a parent applying for their child information where the information relates to their child having provided an account which can possibly be used as evidence to prosecute that same parent with regards to a domestic violence matter). According to the specific circumstances surrounding the request and if a risk of harm is identified, the caseworker will assess whether there is the need to contact the child directly and verify that they are actually aware of the request having been submitted by one of their parents and in case they are the caseworker will look into the option of whether different arrangements can be made for the information to be disclosed to the child directly or whether an exemption applies for the information not to be disclosed at all.
Step 4 – Consider ROARs submitted for vetting/character enquiry checks
Right of access is a specific right under the DPA which allows individuals to request access to the personal data the MPS may hold about them. As a process it should not be used in place of employment vetting or other similar purposes. This is because there are no vetting/ background checks or review involved in the ROAR

process, only disclosure of what personal data is actually held. Consequently no assurance can be provided or inferred as to someone's identity or character on that limited basis. In particular all internal vetting enquiries should therefore be addressed or re-directed to the MPS Vetting Unit and not the DRU.

If an applicant has any further queries about the DPA ROAR application process or general data protection concerns they should email the Administration Team to: MPSDataOffice@met.police.uk

Processing Right of Access Requests (ROARs)

Step 1 – Consider the statutory time period for processing ROARs

By law, ROAR applications must be processed and the personal data to be disclosed posted to the applicant within a maximum period of one calendar month. As a consequence it is important to forward all such applications to the DRU immediately following receipt.

For reference: the applicable time period per DPA begins at the latest of the following:
(a) When the controller receives the request;
(b) When the fee (if any) is paid; and
(c) When the controller receives the information (if any) required under subsection (5) in connection with the request.

The UK GDPR states the time limit should be calculated from the day after the request for access is received until the corresponding calendar date in the next month. If the following month is shorter (and there is no corresponding calendar date), the date for response is the last day of the following month. If the corresponding date falls on a weekend or a public holiday, the next working day is the deadline to respond.

Whilst the DRU always strives to provide requested information as quickly as possible it is to be expected that some ROARs will take the maximum one calendar month to process from the date recorded on the acknowledgement letter. Due to the high number of applications the DRU receive and in the interests of fairness and efficient processing, all applications are processed in the strict order in which they are received.

If the applicant's 'home address' changes during this period, posting to a new address can be arranged, providing the applicant encloses a letter of authority signed by them, detailing where they would like the reply to be sent to and including relevant dates as necessary.

If applicants have not heard anything after one month they should be advised to contact the DRU directly or you can do so on behalf of the applicant. The Mailbox to address this enquiries to is MPSDataOffice@met.police.uk

Step 2 – Helping the DRU Caseworker to find personal data held locally

The DRU can access most MPS ICT systems and information record collections in order to deal with ROARs. However, there will be occasions when they may need to contact Basic Command Unit (BCU) personnel directly to help trace or verify personal data.

If you receive an email or call from a DRU caseworker, you must respond within 3 days of its receipt and provide the information that has been requested. Even if you do not have the requested information you should still reply within 3-days explaining why you do not have the requested information, as the 'clock' will have already started in respect of the statutory time limit to answer the application.

Step 3 – Providing the DRU with permission to release personal data

Permission to Release (PTR) is a process used by the DRU to ask BCUs whether or not there are any specific facts to consider prior to providing the personal data requested by the applicant. For example, it could concern a criminal case that has yet to be heard at court; or there is an outstanding disciplinary investigation; or disclosure could adversely impact the MPS' ability to carry out future law enforcement action. In these situations the onus is on the BCU to flag any concerns/objections and provide justifiable reasons in favour of non-disclosure at this time.

All PTR requests are emailed with automated read receipts and MUST be responded to within 3-days of them being read. A failure to do this will result in the non-compliance being raised with a senior officer at your BCU.

Step 4 – Providing MPS personnel with copy HR record or their personnel file

All MPS personnel must raise a service request under MyHR Self-Service [or telephone [redacted]] for direct access to their own personnel file, which they are generally allowed to access. But, if they wish to pursue a ROAR due to other personnel records that are believed to exist they should follow the same process as required of the public [see above]. MPS personnel can also request their information by emailing the DRU at MPSDataOffice@met.police.uk along with their proof of ID, which can simply be a scanned version of their warrant card. They need to specify whether they would like their disclosure to be sent electronically to their work email address or sent via post to their home address.

Step 5 – Requests to release crime and Connect reports to members of the public

There is no automatic right to receive Connect or CRIS reports on request. They are not routinely provided and can only be released upon receipt of a valid ROAR from the victim/other individual directly involved e.g. a witness. As with any ROAR the normal application requirements apply as previously described [i.e. made in writing and submitted with proof of ID] and forwarded to the DRU to process. When supplying a copy of any Connect or CRIS report, the MPS reserves the right to withhold or redact certain details. This could include personal data relating to other persons recorded in the Connect or CRIS report, or any identifying/confidential data that could interfere with ongoing investigations/other policing purpose if released.

Other data subject rights under the DPA

Part 3, Chapter 3 of the DPA 2018 Act provides the following individual rights:

Right to be informed

It is about providing individuals with clear and concise information about what you do with their personal data.

This type of information is included in a document called the Privacy Notice. To view the MPS Privacy Notice please follow the link below:

https://www.met.police.uk/search?q=privacy+notice

Right to rectification

Individuals have the right to have inaccurate personal data rectified which include being able to have incomplete personal data completed. This does depend on the purposes for processing and it may involve providing a supplementary statement to the incomplete data. If you become aware that a member of the public wishes to submit a request for rectification of data please provide the Disputes form to them, you can access it by searching for Data Disputes form V4 on the forms section of the intranet, and advise them to fill it in and send it together with a valid proof of ID and a proof of address dated within the last 6 months to the Data Office to: MPSDataOffice@met.police.uk

Right to erasure and Right to restriction

Individuals have the right to have personal data erased. The right is not absolute and only applies in certain circumstances. Specifically in regard to data collected and processed for policing purposes the application of this right is limited to a narrow range of circumstances:

- Accuracy of the personal data is contested
- Processing is unlawful
- MPS no longer needs the personal data for the purposes of processing
- The data subject has objected (once it has been verified that the data subject's rights override MPSs legitimate grounds for processing the data). See Article 2 of the GDPR for further guidance and information.

A data subject can request the MPS to restrict or stop processing their personal data. Under DPA this type of request must be considered and responded to within one calendar month of it being received. Therefore, if an individual has told you to stop using their personal data you should contact the Data Office by writing to MPSDataOffice@met.police.uk

Right not to be subject to automated decision-making

The purpose of this right is to provide safeguards for individuals against the risk that a potentially damaging decision is taken by solely automated means, i.e. without

human intervention however currently, solely automated decision-making that leads to an adverse outcome is rarely used in the law enforcement context and is unlikely to have many operational implications.

It is to be noted that the above listed rights are the rights of a data subject which an organisation which collects and process data for law enforcement purposes needs to adhere to and they are contemplated by Part 3, Chapter 3 of the DPA. They are five rights. The rights contemplated by the UK GDPR are eight and are the general data subject rights, in addition to the five above mentioned rights the data subject has also the following rights: The right to data portability, right to object, other rights in relation to automated decision making and profiling. These do not apply to information held for policing purposes but would instead apply to personal information held for purposes other than policing such as information held by HR or OH for instance.

Requests for deletion of information on Police National Computer and of IMAGES and/or BIOMETRIC DATA

Any requests for deletion of information on Police National Computer (PNC) and for deletion of images and/or biometric data (i.e. DNA, fingerprints) are within the remit of the Record Deletions Unit (RDU) however requests will need to be submitted by the applicant via the National Police Chief's Council's (NPCC) ACRO department who may then cascade some of the requests to the individual police forces' units.

ACRO's contact details:

Post: ACRO Information Management Unit, PO Box 481, Fareham, Hampshire, PO14 9FS
Email: [redacted]
Link to ACRO website: https://www.acro.police.uk/
Link to ACRO website Records deletions section https://www.acro.police.uk/Services/Record-deletion

Requests for deletion of information on MPS systems other than PNC (including disputes related to the accuracy of data held on PNC)

These requests will need to be forwarded on to the Data Office and confirm to the member of the public that their request had been forwarded to the Data Office where the Data Disputes Manager will be looking into their request and will contact them directly.

To summarise regarding Right to Erasure requests and Right to rectification requests:

RDU via ACRO deal with deletions of:
- PNC entries
- Images
- Biometric data

DPA Disputes Manager in the Data Office deals with:

- Corrections of PNC of inaccurate data related to either personal information or convictions etc.
- Correction and/or deletion from Connect and other legacy systems such as CRIS, CRIMINT and more where possible.

Information Management Support

Data Protection is a very wide area and this guide provides information and guidance around data rights, types of disclosure and data breaches. The support page linked below provides knowledge and guidance on other data protection topics.

On the support page you can find digital tiles which give you access to MPS policies around management of data, including the MPS Privacy Notice, information and policies related to individuals' rights regarding data and around information sharing, data protection impact assessments, records management and information security.

You can access the support page by clicking on its link "Information Management" at the top of this guide above the title and next to the "support" link or if you wish to access it separately the link is the following
: [redacted]

Disclosure of personal data to third parties

Position regarding MPS release of third-party details to individuals/solicitors

Under DPA Schedule 2, Part 1 Clause 5(3)(a)(b)(c), the MPS can also release personal information "where the disclosure of data:
- is necessary for the purpose of obtaining legal advice, or
- is otherwise necessary for the purposes of establishing, exercising or defending legal rights.

The MPS can release some personal information relating to a data subject to third parties, but only if the MPS is adequately satisfied it is required for legal proceedings or proposed legal proceedings.

Requests under DPA Schedule 2, Part 1 Paragraph 5, Art. 3 (a)(b)(c) are dealt with by the relevant BCU and are most likely to be in connection with civil actions which are underway or in contemplation. Proof of the intended legal proceedings must be requested from the applicant.

It is important to note that just because the MPS has received a Schedule 2, Part 1, Paragraph 5, Art.3 (a)(b)(c) request, unless it is a Court Order, the MPS is not obliged to disclose the requested information. The following steps are to be followed in the decision making process:
- the first test is that an officer of sufficient authority [i.e. Inspector or above] will need to risk assess the potential for any foreseeable harm to the data subject or others that may result from disclosing such details
- You should request the information you require from the relevant Borough Commander (at your local police station) where the incident occurred. Please note, the release of the material is at the discretion of the Borough Commander.

- the public interest in a victim/ witness or other individual being able to pursue a claim for compensation/ legal redress must also clearly outweigh any duty of confidentiality already owed to an individual under DPA provisions, such as a suspect [i.e. *the data subject*] and
- whatever decision is made that fact and the rationale for such an outcome must be appropriately recorded on Connect in case reasons to disclose or withhold are later challenged
- in the event of you having any concerns about the safety of disclosing requested information, advice can be obtained from the Data Rights Unit. Please note the DRU is unable to make the decision for you but they can be consulted to ensure you are following the process appropriately
- if the MPS has received a Court Order the MPS is obliged to disclose the information. All Court Orders must be forwarded immediately to the DLS a [redacted]

Position regarding release of Connect or CRIS reports to insurance companies:

Connect/CRIS reports can only be released to insurance companies under the Memorandum of Understanding (MoU) between the NPCC and the Association of British Insurers (ABI). Once they pay an appropriate fee and send in an Appendix D(a) or D(b) document to the DRU.

If the company suspects fraud, they must also provide written evidence and send it together with a completed Appendix E document to the DRU justifying release of personal data relating to their insured. Applications where fraud is suspected are processed free of charge.

Other requests for personal information

Applicants who need a 'Police clearance certificate'/ 'Certificate of good conduct' for a visa or emigration purposes

The UK police do not issue either "certificates of good conduct" or "police clearance certificates". However, it is the experience of the Data Rights Unit that foreign embassies will generally accept a police reply under DPA right of access provisions as a suitable equivalent.

Individuals requiring Police Certificates for the purposes of emigration, visas, work permits should alternatively download the application form for an NPCC ACRO Police Certificate directly from the ACRO website.

Please note that Police Certificates are processed entirely by the NPCC ACRO Criminal Records Office.

All submissions and enquiries from the public relating to this process should be directed to ACRO, who can be contacted through the following routes:
- Telephone: 02380 479 920 [during their office opening hours of 8:30 – 23:00, Monday to Friday]
- E-mail:customer.services@acro.pnn.police.uk
- Address: ACRO, PO Box 481, Fareham, PO14 9FS

This form must be returned to NPCC ACRO; it must not be returned to the MPS.

Applicants who need a 'Police clearance certificate' or 'Certificate of good conduct' in respect of their employment

The MPS do not provide PNC disclosures for employment vetting purposes. If the applicant requires a disclosure for employment purposes, they should contact Disclosure Scotland by post at PO Box 250, Glasgow, G51 1YU, telephone: 03000 2000 40 or via their website: Disclosure Scotland.

It is a criminal offence for an employer to ask individuals, as a condition of employment, to request this information under a right of access request under a practice known as 'enforced right of access'.

However, if the applicant is going to work as a paid employee or as a volunteer for an organisation, involving work that will bring them into contact with children or vulnerable adults, they are required to undergo a Disclosure and Barring Service (DBS) check. In such circumstances subject access does not provide an appropriate level of assurance and applicants must therefore access the DBS website and follow their procedures.

Applicants who request personal data for an employment tribunal involving the MPS

Right of access is also not an appropriate way to obtain information for individuals considering or taking the MPS to an employment tribunal. The right of access provisions will only provide limited information that will be redacted to ensure no other third party personal data remains, even if that data was relevant to the case. The court/ tribunal might also not see information refused due to the application of DPA exemptions. Like other courts/ tribunals, employment tribunals have a more complete process whereby the parties follow a mutual stage of information/ evidential disclosure or 'discovery' stage covered by pre-court procedures and this is the appropriate way to obtain 'personal data' and any other relevant information the parties require for open court/tribunal proceedings. The tribunal will also have the power to give extra directions or orders on this and other matters relating to disclosure during hearings, which the MPS/claimant must follow.

Please note - Court Orders served on the MPS must be forwarded immediately to the DLS.

Breaches of the DPA and role of the Information Commissioner

Breaches of the DPA and role of the Information Commissioner

All MPS personnel and partners who access/process MPS information need to be aware that breaches of the DPA provisions are reportable under the MPS Security Incident Reporting scheme and the online form can be accessed via the link below:
[redacted]

Data Protection breaches are breaches in relation to personal data for which MPS (the data controller) is responsible and likely to result in risk to the rights and freedoms of individuals.

Under DPA the MPS's Data Protection Officer (DPO) is obliged to report significant data protection breaches to the Information Commissioner's Office (ICO) on behalf of the Data Controller [i.e. the Commissioner] within a strict time scale of 24 hours from when the breach occurs. The notification must outline:
- Name and contact details of who is making the report
- Date and time of the breach (or an estimate);
- Date and time it was detected it;
- Basic information about the type of breach; and
- Basic information about the personal data concerned.

The ICO breach notification form needs to be used. It is possible to attach documents to the form if necessary.

If possible, you should also include full details of the incident, the number of individuals affected and its possible effect on them, the measures taken to mitigate those effects, and information about your notification to the data subject. If these details are not yet available, you must provide them as soon as possible. You must submit a second notification form to the ICO within three days, either including these details, or providing an estimate of how long it will take you to get them.

Failure to submit breach notifications can incur a £1,000 fine.

The introduction of DPA [incorporating the new GDPR and Law Enforcement Directive] on 25 May 2018 means all public and private sector organisations who lose or compromise personal data they hold, will be subject to a significant increase in penalties. For public sector bodies i.e. the MPS and other police forces, this will relate to fines potentially of up to €20 million.

Criminal offences under the DPA – There are a range of offences relating to data protection legislation that can involve data controllers, data processors and others in receipt of personal data, which are highlighted below:

WARNING:
Anyone who knowingly discloses the personal data of another person without either that person's consent or other legal authority is at risk of prosecution under the DPA. Dependent on circumstances other offences, such as under the Computer Misuse Act 1990 may be relevant.

It is also an offence to alter, deface, block, erase, destroy, or conceal personal data for example in order to prevent disclosure on receipt of a right of access request or other application under the DPA.

MPS personnel will also undoubtedly face disciplinary action in circumstances where they have deliberately disclosed personal data and that could result in dismissal from office. As previously stated all MPS personnel owe a duty of confidentiality to the

Commissioner [as data controller] so they must also take due care in processing personal data as directed to avoid making mistakes.

It is therefore important that all MPS personnel and partnership staff etc. follow the MPS's Information Code of Conduct and instructions in this document to ensure they process personal data legally and with care strictly in accordance with their policing role. Anyone who drops below the standard of conduct required and who loses or compromises personal data, could also face disciplinary action.

Feedback

We would like you know your thoughts on the Data Protection Act policy guidance.
Did you find this policy guidance useful?

Yes ☐ No ☐

Please tell us how we can improve this page.
Please enter feedback

Thank you.