METROPOLITAN POLICE Working together for a safer London

Freedom of Information Act Publication Scheme	
Protective Marking	Not Protectively Marked
Publication Scheme Y/N	Yes ☒ No☐
Title	Data Protection Act 1998 (DPA) - Compliance Standard for International Data Processing Standard Operating Procedures (SOPs)
Version	Version 1.0
Summary	The purpose of this document is to define the minimum standard operating procedures to be applied by MPS officers and staff in order to support compliance with the DPA 1998 when processing data internationally.
Branch / OCU	Directorate of Information, Information Management DoI2 (3-3)
Date created	March 2011
Review date	March 2014

Data Protection Act 1998 Compliance Standard for International Data Processing - Standard Operating Procedures (SOPs)

Table of Contents

---

1. INTRODUCTION

These standard operating procedures (SOPs) support the MPS Information Management Policy.

The very nature of police work often leads to working with partners internationally in preventing/tackling crime and acts of terrorism. To do this requires acceptance and sharing of information which includes processing personal information held by the Metropolitan Police

Service (MPS) across international borders. Such processing is governed by the requirements of the Data Protection Act 1998 (referred to as the Act or DPA) and international agreements, which all personnel must abide by to ensure the processing is fair and lawful. Any specific definition of personal data and sensitive personal data can be found in the 'Processes for Data Protection Act 1998 Compliance SOPs, sections 4 and 5'.

1.1 Application

All police officers and police staff, including the extended police family and those working voluntarily or under contract to the MPA must be aware of, and are required to comply with, all relevant MPS policy and associated procedures.

However, this SOP applies in particular to officers and staff in the following roles, ranks and grades:

- Borough Operational Command Unit (BOCU) Commanders;
- OCU commanders;
- Heads of branches;
- Chief Inspectors and Police Staff at Band C or equivalent;
- DoI2 (3-3) Public Access Office personnel;
- The MPS Data Protection Officer (DPO), and
- Other MPS personnel, particularly in central departments, with responsibility regarding transferring personal or sensitive personal data internationally.

N.B. This list is not intended to be exhaustive.

These SOPs apply in particular to officers and staff who have defined responsibilities for ensuring that they and their personnel are appropriately briefed on the application of data protection legislation plus the sharing and processing of personal/sensitive personal data across international boundaries.

In particular due to corporate responsibility and the potential legal complexities involved, it is expected that any international data processing is authorised in advance by at least the level of Chief Inspector or Police Staff Band C level or equivalent. This must then be signed-off as appropriate by Operational Command Unit (OCU) Commander. It should be noted that for some transfers of crime intelligence personal data outside the European Economic Area (EEA) (for further details see section 6), the authority of a Superintendent is required (see the

relevant Serious Organised Crime Agency, SOCA protocols). Otherwise so long as these authorities are in place, the mechanisms for actually transferring personal data internationally can be delegated to other personnel.

1. 2 Scope

These SOPs do not replace existing practices of sharing personal information internationally. Neither do these SOPs introduce any further level of bureaucracy or interfere unduly with situations where established processes for international data processing already exist. So long as data protection requirements are considered in a similar manner to the human rights provisions for individual data subjects, referral to these SOPs will generally be supplementary to existing protocols between the MPS and other law enforcement agencies, both home and abroad.

Examples include arrangements with Interpol or Europol, which is normally managed by the Serious Organised Crime Agency (SOCA); or other agencies such as the Association of Chief Police Officers Criminal Records Office (ACRO) and the UK Central Authority for the Exchange of Criminal Records (UKCA-ECR). International data processing is likely to exist in scenarios such as extradition or where crime intelligence is disseminated overseas by the Met Intelligence Bureau (MIB) under Home Office and international arrangements.

Where there is a need to share information with our international crime prevention partners then MPS personnel should first consider and seek advice on sharing data internationally via such established methods:

- For advice on sharing information via Interpol or Europol (e.g. wanted persons) and processes relating to International Letters of Request (also known as *Commission Rogatoire*), you should contact the SCD6 International Assistance Unit.
- Furthermore, under European law, combined with s.144 of the Coroners & Justice Act 2009, there is also a requirement since 15 August 2010 for greater sharing of criminal convictions and intelligence across the European Economic Area (EEA). See the list in Section 6. You should contact International Intelligence & Evidence Exchange (IIEE) - TP Operation Emerald in such cases.
- In matters of international terrorism etc., SO15 Counter-Terrorism Command (CTC) and the Security Services should be consulted. For officer briefings and foreign travel see also SO15 Counter-Terrorism Command and SCD14 International Crime Coordination Unit.

N.B. This list is not intended to be exhaustive.

If data protection issues arise in the course of any of these areas of international data sharing, the specialist units concerned are responsible for obtaining advice directly from the MPS Data Protection Officer (DPO). The DPO will in some cases refer the matter to the Directorate of Legal Services (DLS). Alternatively in 'live' criminal cases there will probably be a requirement for legal advice from the prosecuting authorities such as the Crown Prosecution Service (CPS).

1.3 Purpose

These SOPs describe in detail what is required to allow personal data to be transferred across international borders. The central tenet is that processing of personal data internationally must be carried out legally (in accordance with DPA 1998 Principle 8) and in a secure manner (in accordance with DPA 1998 Principle 7).

These SOPs focus specifically on the **7th principle** (adequate security) and **8th principle** (adequate protection for the rights and freedoms of individuals requirements in relation to international data processing). Instances of international transfers of personal data must be recorded using approved systems/processes for the purposes of future inspection and audit.

It is assumed throughout these SOPs that the Directorate, OCU or BOCU intending on transferring personal information internationally has satisfied themselves in advance that the processing is compliant with Principles 1 to 6 of the Data Protection Act 1998 and with the purposes registered by the MPS under the Act [see Data Protection Act 1998 (DPA) Compliance SOPs section 9.1 and link in **Appendix B**]. Further guidance on this can be obtained from the MPS Public Access Office.

There are instances where it is not appropriate to share data via Europol or Interpol or under established arrangements (see section 1.2) and these SOPs cover these circumstances. An illustration is that where the right circumstances apply, besides police information (i.e. crime related information and intelligence); other MPS organisational information, including personal data, can potentially be transferred internationally. This assumes that the requisite legal and security safeguards are in place.

1.4 Role of the Data Protection Officer

The MPS Data Protection Officer (DPO) or MPS Deputy Data Protection Officer (DDPO) **must** be notified where there is an intention to transfer personal data internationally outside of the Interpol and Europol process **before** the transfer takes place. Instances where

consultation **must** also take place is where there is an intention to process or transfer large bulk personal or sensitive personal data either as a one-off or long term arrangement.

In all circumstances regarding the Data Protection Act 1998 and associated legislation, business groups **must** initially seek the advice of the DPO or DDPO where there are any doubts or questions as to how to proceed with processing personal data. This includes international data transfers and is always undertaken **before** any approach is made to the Directorate of Legal Services (DLS) for specialist legal advice. If legal advice is required the DPO will make that assessment and submit an informed request for specialist data protection legal advice to the DLS.

1.5 Quick Reference Flow Chart

To assist readers of these SOPs there is a quick reference flow chart in **Appendix A**, taking readers through the process of establishing whether personal data can be lawfully transferred internationally. However, readers must familiarise themselves with the remaining contents of these SOPs to ensure all aspects relating to lawful processing have been considered.

2. IS IT NECESSARY TO SEND PERSONAL DATA?

Before embarking on the process of determining the appropriate avenues to take in order to process personal data internationally, it is important to first consider whether personal data is needed at all. Could the data be suitably anonymised so it will not identify living individuals and therefore not engage the constraints of the Act. This will allow the free transfer of such data outside of the European Economic Area (EEA). It must be remembered that the removal of an individual's name does not in itself anonymise data. Refer to the Data Protection Act 1998 Compliance SOPs for further guidance on what constitutes personal data or sensitive personal data.

3. THE ADEQUATE PROTECTION OF THE RIGHTS AND FREEDOMS OF INDIVIDUALS - 8th DATA PROTECTION PRINCIPLE

The Data Protection Act 1998 (the Act) states:

"*Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data."*

There are a number of avenues that allow the MPS to transfer personal data internationally which will meet the above requirement. In order to establish the most appropriate avenue to

take first define what is a data 'transfer' and what is considered to be data 'in transit'. What also needs to be established is whether the transfer is for the purposes of a data processing arrangement between the MPS as Data Controller and the international partner as a data processor or whether the transfer is to another data controller. The definitions of the words 'transfer' and 'transit' are important to determine which international laws apply, the liability of the MPS and what the Act and the EU Data Protection Directive requires of the MPS.

4. WHAT IS A DATA TRANSFER?

From the outset, it should be noted that the definitions stated here relating to 'data transfer' and 'data transit' are in the context of the application of the legislation to international data processing. Technical definitions relating to electronic/systems transfer of data may differ from this interpretation in some circumstances.

The Act does not define what is considered to be 'data transfer'. However, in the absence of a definition the Information Commissioner's Office (ICO) has defined a transfer as "*sending personal data to someone* or to an organisation *in another country*".

Data transfer does not mean the same as mere transit. Therefore, the electronic transit of personal data routed through country 'A' whilst in transit to country 'B' does not constitute as a data transfer to country 'A'.

It's important to note that a transit becomes a transfer if the data is processed by the holding country at any point. See section 6 of the 'Processes for Data Protection Act 1998 Compliance SOPs' for more information regarding data processing. If you are unclear as to whether the data is 'in transit' or is 'transferred' please consult with the MPS Public Access Office or DoI2 (3-1) Information Assurance Unit for further guidance.

4.1. Uploading Data on the MPS or Other Websites

The MPS uses an array of media tools to connect with members of the public for the purposes of prevention and detection of crime and the apprehension or prosecution of

offenders. This includes the use of the MPS internet site or other websites, such as 'YouTube' and 'Flickr' to appeal to members of the public for further information regarding suspects of crimes e.g. 'London's Most Wanted' or 'Caught on Camera' or keeping members of the public informed of the recent convictions of criminals or the issuing of Anti Social Behaviour Orders (ASBOs).

The uploading of personal data on to websites will more often than not result in transfers to countries outside the European Economic Area (EEA) due to the content being automatically made available to anyone who has access to the Internet anywhere in the world. The transfers will take place when someone outside the EEA accesses the website. Therefore, there has to be a significant public interest in the publishing of such data using the World Wide Web and such justifications must be approved by the operational Chief Inspector and recorded on the CRIMINT system. Additionally, the data must be removed from all websites once the policing purpose no longer exists and confirmation of this removal must also be documented on the CRIMINT system.

Example 1: A public appeal for information to identify a suspect caught on CCTV

Once a suspect is positively identified the footage **must** be removed within two calendar months from all websites on which the MPS has published the footage. It is accepted that the MPS are unable to control the republishing of this data on other websites, which is why the publishing of CCTV footage or imagery should only be done for crimes which attract significant public interest justifications (e.g. CCTV footage used within a public appeal to identify a suspect of a sexual assault).

For further guidance on the release of images of this nature please refer to the 'ACPO Media Guidance on the Release of Images of Suspects and Defendants' (see additional link at ACPO Media Centre), for more detailed advice on specific processing measures needed in order to publish this information fairly and lawfully. It may also be useful to refer to the joint protocol between ACPO and CPS on Publicity and the Criminal Justice System.

Example 2: The Publishing of Details of Recently Convicted Criminals or the Issuing of ASBOs

There are a number of initiatives which raise awareness and understanding of what the public can expect from the police and other agencies, with regards to reducing crime and seeking justice. This includes making sure local priorities are tackled and demonstrating that

there are tough, visible consequences for those who break the law. The initiatives include the publishing of details regarding recent convictions and the issuing of ASBOs. It is important that such disclosure is proportionate to the crime committed and the conviction given, whilst also bearing in mind factors such as the age of the offender and what is considered to be a sufficient level of disclosure to meet the purpose of keeping the public informed without breaching the Human Rights of the offender.

For further and more detailed guidance on the publication of ASBOs please refer to the 'Home Office Guidelines on the Publishing of ASBOs'. For further details on the MPS use of CCTV and the DPA requirements refer to the Processes for Data Protection Act Compliance SOPs at 13.1.6.

Further and more specific guidance around the publishing of personal data on the MPS websites can be obtained from the Public Access Office.

4.2 The Use of MPS Laptops and Smart Phones (Blackberries etc.) Internationally – Is It A Data Transfer?

International operational demands require MPS personnel to have real time access to MPS systems worldwide. There is a simple method to determine whether the processing becomes international or whether it remains within UK jurisdictions which is as follows:

Figure 2.1 - Scenario A:

An employee accesses documents on the MPS network via her approved MPS laptop whilst she is visiting the USA. It is only the employee which has access to this information and she does not allow anyone else to access it. This includes emails, printouts or showing the onscreen information to her USA counterparts, either deliberately or accidentally such as someone else looking over her shoulder. In these circumstances, the information is not considered to be transferred and remains under UK protection.

Figure 2.2 - Scenario B:

An employee accesses documents on the MPS network via his approved MPS laptop whilst he is visiting the USA. As part of the international coordination effort between the MPS and our US counterparts the employee imparts some of the information he has on his laptop to our FBI colleagues. At the point of the employee sharing the MPS information with the representative of the USA, the information is considered to be internationally transferred.

Some countries have strict import/export custom regulations regarding the transportation of laptops across their borders and may demand access to the laptops to scan for malicious or suspicious content. When such access is given, this becomes an international transfer. Therefore, it is important for staff members to plan ahead to ascertain whether special dispensation from the customs checks can be granted by the relevant international authority or to take the necessary actions laid out in these SOPs to enable the fair and lawful transfer of this information internationally.

Reference should also be made to restrictions on the use of encryption internationally as METSEC Code TEC4 Encryption (see METSEC Code (MPS Security Manual) refers. Briefings are provided to officers before going abroad from the SCD International Crime Co-ordination Unit.

5. IS THE TRANSFER TO A DATA PROCESSOR OR A DATA CONTROLLER?

Establishing whether the transfer of the data is to a 'Data Processor' or 'Data Controller' is important in order to ascertain whether specific contracts or agreements are needed. Specific contracts/ agreements are needed when transferring data internationally to ensure that the MPS Commissioner, as overall data controller, is not held liable for any breaches in the Act. The definitions of both are as follows:

Data Controller: A person who, either alone or jointly or in common with other persons, determines the purposes for which and the manner in which any personal data is, or is to be, processed.

As the Data Controller for the MPS the Commissioner of Police of the Metropolis determines 'how, what, when, why and where' rules around the personal data which the MPS processes. The Commissioner of Police of the Metropolis takes the overall responsibility for whatever happens to the data processed by the MPS, therefore, is liable for breaches of the Act, criminal offences, civil proceedings and Information Commissioner's Office enforcement action.

If the data is being transferred to a Data Controller, staff members have three options to pursue to ensure the lawful transfer of this data which are covered in more detail in section 8 of these SOPs.

Data Processor: Any person, other than an employee of the data controller, who processes the data on behalf of the data controller.

For example, the MPS has outsourced its pay and pensions processing to 'Company A'. 'Company A' processes the personal data of MPS employees on behalf of the Commissioner

of Police of the Metropolis. However, 'Company A' does not determine the 'how, what, when, why and where' rules as 'Company A' follows the rules set by the Commissioner. Therefore, 'Company A' is deemed to be a Data Processor.

Increasingly police forces are looking for more efficient models of conducting policing business and data processing arrangements are being more widely sought due to the cost savings they usually present. It is not uncommon for large private sector corporations to outsource data processing to countries such as India. This is known as off-shoring. However, this is not generally the case for police forces due to the sensitive nature of the data we process and off-shoring will only be considered if properly managed.

In limited circumstances international data processing arrangements may be established. However, advice **must** always be sought from the Data Protection Officer **before** any decision is taken to proceed.

If the data is being transferred to a Data Processor a Data Processing Agreement will need to be established, which must incorporate the EU model contractual clauses. You should refer to section 8.2 of these SOPs for further guidance. Business Groups should note that the MPS Commissioner is still legally responsible for making sure that the data is processed in line with the Data Protection Act 1998 principles. In particular, personal data can only be transferred if there is a contract binding the processor to have appropriate security and to act only on MPS instruction. The personal data should continue to be protected to the same standard as in the UK which includes the protection of the rights and freedoms of data subjects. When selecting a data processor, Business Groups need to satisfy themselves that the processor is reliable and has appropriate security, which has been considered and approved by the DoI2 (3-1) Information Assurance Unit.

6. PROCESSING PERSONAL DATA WITHIN THE EUROPEAN ECONOMIC AREA (EEA)

The transfer of personal data to the following EEA countries has no restrictions under Principle 8 of the Act:

Austria	Latvia
Belgium	Liechtenstein
Bulgaria	Lithuania
Cyprus	Luxembourg
Czech Republic	Malta

Denmark	Netherlands
Estonia	Norway
Finland	Poland
France	Portugal
Germany	Romania
Greece	Slovakia
Hungary	Slovenia
Iceland	Spain
Ireland	Sweden
Italy	

Data transfers within the EEA must be treated with the same careful handling as we would apply to transfers between our partners in the UK. This includes, but is not limited to, ensuring that the recipient is registered with their local Data Protection Supervisory Body and that the transfer is in line with our policing purposes.

On occasions the MPS may transfer personal data to UK Government facilities such as UK embassies or consulates. These are considered to be UK territory and are therefore not considered to be transfers beyond the EEA.

7. PROCESSING PERSONAL DATA OUTSIDE OF THE EEA, BUT WITHIN A EU APPROVED 'SAFE COUNTRY'

If there is a need to transfer personal information outside of the EEA there are a small number of countries which the European Commission has assessed as having data protection regimes that it considers provide the level of adequacy required to transfer data safely. The countries which are considered to be safe are:

Argentina	Faroe Islands
Canada	Switzerland
Guernsey	Principality of Andorra
Isle of Man	Israel
Jersey	USA*

*United States of America, *but only to organisations which are registered under the "Safe Harbor" scheme – see* ***Section 7.1***

As with Data transfers within the EEA, data transfers to 'safe countries' must be treated with the same careful handling as we would apply to transfers between our partners in the UK.

7.1 Processing Personal Data within the USA

Although the United States of America (USA) is not included in the European Commission list, the Commission considers that personal data sent to the US under the 'Safe Harbor' scheme is adequately protected. When a US company signs up to the 'Safe Harbor' arrangement, they agree to:

- follow seven principles of information handling; and
- be held responsible for keeping to those principles by the Federal Trade Commission or other oversight schemes.

Staff members **must note** that 'Safe Harbor' only applies to registered private sector companies and does not extend to the public sector, which includes the US law enforcement agencies. Therefore 'Safe Harbor' cannot be relied upon where there is an intention to transfer personal data to our US law enforcement partners. However, the transfer may still take place using the transfer options detailed within Section 8 of this SOP.

To view a list of the private sector companies signed up to the 'Safe Harbor' arrangement refer to the US Department of Commerce website - US Department of Commerce website.

8. PROCESSING DATA INTERNATIONALLY OUTSIDE OF THE EEA AND APPROVED COUNTRIES

Countries which are not within the EEA or assessed by the EU as an approved safe country are termed 'third countries' and will be referred to as such throughout the remaining part of these SOPs.

The MPS is able to process personal data within 'third countries' by ensuring that there is an adequate level of protection of the personal data once transferred by:

- **Option One** - conducting an adequacy self assessment;
- **Option Two** - using contracts, including the European Commission approved model contractual clauses; or

- **Option Three** - relying upon the exceptions from the rule.

The relevant adequacy process to undertake depends very much on the nature and urgency requirements of the data processing. For example, where there is an urgent international operational law enforcement requirement, such as national security or life/death matters, the adequacy self assessment and the drawing up of contracts is likely to be too slow a process in order to address the urgency of the operational need. Therefore, employees are advised to refer to Section 8.3 for advice on Schedule 4 exceptions. For other requirements such as procurement, data processing, or long term or low urgency policing objectives, employees should either undertake the adequacy self assessment (**Option One**) or use the EU approved model contractual clauses (**Option Two**). Project specific guidance around the most appropriate process to undertake **must** be sought from the Data Protection Officer or Deputy Data Protection Officer.

8.1 Option One: Conducting 'Adequacy of Protection' Self Assessments

Assessing 'adequacy of protection' within a 'third country' has two stages:

1 – General Adequacy Assessment (GAA)

2 – Legal Adequacy Assessment (LAA)

Both of these stages need to be carried out in order to make a full assessment of the risk posed to both the MPS Commissioner and the Data Subject to make an informed judgement around the viability of undertaking an international data transfer with minimal risk. However, if the data intended to be transferred is of low risk, such as transferring of internal contact details of staff members not based in operationally sensitive areas, then only a GAA will need to be completed. Guidance from the Data Protection Officer **must** be sought to ascertain what the appropriate assessments to make are.

Staff members **must** note that the level of protection is unlikely to be adequate if:

- the transfer is to a processor in an unstable country; and
- the nature of the information means that it is at particular risk, including risks around the third country's poor human rights record.

In such circumstances where there is a substantial public interest to proceed with the transfer, such as the processing being in the interests of national security, then staff members are advised to proceed to **Options 2 or 3** and seek the advice of the Data Protection Officer or the Deputy Data Protection Officer.

8.1.1 General Adequacy Assessments (GAA)

The GAA is the simpler of the two assessments to undertake as the knowledge required to make this assessment should either be already held by the MPS or is easily obtained. These are:

- the nature of the personal data;
- the purpose(s) of the proposed transfer;
- the period during which the data is intended to be processed;
- any security measures taken in respect of the data in the third country;
- the country of origin of the personal data; and
- the country of final destination of the personal data.

A GAA grid can be found in **Appendix B**. Advice on the completion of this can be obtained from the (Deputy) Data Protection Officer. Once the GAA is completed the next step to take is the LAA.

8.1.2 Legal Adequacy Assessments (LAA)

In assessing the LAA consideration must first be given to the following:

- the law in force in the third country;
- the international obligations in that third country; and
- any relevant codes of conduct or other rules which are enforceable in that country or territory.

In addition to the above, Business Groups should consider the following questions:

- Has the 'third country' adopted the Organisation for Economic Co-operation and Development (OECD) Guidelines on the Protection of Privacy and Transborder Flows of Personal Data and, if so, what measures has it taken to implement them?
- Has the 'third country' ratified the Council of Europe Convention for the protection of individuals with regard to the automatic processing of personal data (Strasbourg 1981) and are there appropriate mechanisms in place for compliance with it?
- Does the 'third country' have a data protection regime in place which meets the standards set out in the Article 29 Working Party document (Pages 5 -7) (Transfers of personal data to third countries: Applying Articles 25 and 26 of the EU data protection directive) adopted on 24 July 1998 (WP 12).

- Does the 'third country' have any legal framework for the protection of the rights and freedoms of individuals generally?
- Does the 'third country' recognise the general rule of law and, in particular, the ability of parties to contract and bind themselves under contracts?
- More specifically, are there laws, rules or codes of practice (general or sectoral) which govern the processing of personal data?

It is expected that the organisation which is intended to receive the data from the MPS should be in the position to answer all of the above questions. It should provide evidence of adherence and compliance with the above guidelines plus standards in order to enable the adequacy assessment to take place.

If adequacy cannot be established either generally or legally, then Business Groups should proceed to **option two**.

8.2 Option Two: Using Contracts, Including the European Commission Approved Model Contractual Clauses

Adequacy of protection can be secured using a contract between the MPS and the recipient when transferring data internationally. What type of contract depends upon the business need and the type of processing required. The main contractual types are:

- contracts based on the standard contractual clauses approved by the European Commission (EC model clauses); and
- other contracts in which business groups (with the advice of the Data Protection Officer and DLS) create themselves after conducting a risk assessment to bring protection up to an adequate level.

8.2.1 EC Model Clauses

The European Commission has approved three sets of standard contractual clauses, known as model clauses, as providing an adequate level of protection. If Business Groups use the model clauses in their entirety within the contracts between the MPS and the data recipient then the adequacy of protection is automatically granted.

Two of the sets of model clauses relate to transferring personal data from one company to another company, which will then use it for its own purposes. In this case Business Groups can choose either set of clauses, depending on which suits the needs of the business. The other set of model clauses is for transferring personal data to a data processor acting on the

MPS Commissioner's behalf. See Section 5 of this SOP for further guidance on the definitions of 'Data Controller' and 'Data Processor'. If Business Groups are unsure as to which set of model clauses to use refer to the Data Protection Officer or Deputy Data Protection Officer for further guidance.

Links to the model contract clauses:

2004 controller to controller
2001 controller to controller
2010 controller to processor

Business Groups must note that the clauses **cannot be altered in anyway** either by amending, adding, or deleting any elements to change the meaning of the contract.

8.2.2 Other Contracts

It is advisable that Business Groups use the above model clauses when transferring data internationally. However, there may be limited circumstances that require a creation of a contract from scratch. Examples include where there may be particular processing requirements which may not be addressed by the model clauses above or a requirement of the receiving company to return the information after the contract expires.

Whilst separate contracts for data protection are not necessary as the general contract can cover the data protection requirements, in all circumstances the EC model clauses should be used as a reference point as to the minimum standards required to ensure adequacy of protection.

8.3 Option Three: Relying Upon the Exceptions from the Rule (Schedule 4 Derogations)

There are a number of exemptions from the eighth principle which the MPS can legitimately apply to allow the international transfer of personal information. However, whilst these exemptions are available to the MPS to cite there is still a requirement to meet the remaining Principles of the Act to allow the fair and lawful processing of this data. Further guidance on the Principles of the Act can be found within the Processes for Data Protection Act 1998 (DPA) Compliance SOPs.

Any data transfer to a third country must first be risk assessed for likely impact to the individual when the information is transferred. If it is likely that the Human Rights of the individual will be breached if the transfer is made e.g. the likelihood of torture of the individual, or the receiving country is unstable; then it is likely that the processing will not

meet the thresholds for adequacy of protection. Therefore, advice from the Data Protection Officer or Deputy Data Protection Officer must be sought in such circumstances.

8.3.1 Contract performance

The MPS can transfer personal data overseas where it is necessary for carrying out certain types of contract or if the transfer is necessary to set up the contract. For a contract between the organisation and the individual, the MPS may transfer personal data overseas if the transfer is:

- necessary to carry out the contract; or
- a necessary part of the steps the individual has asked the MPS to take before a contract is made between the two parties.

For a contract between the organisation and someone other than the individual, the MPS may transfer personal data overseas if:

- the individual requests the contract or it is in their interests; and
- the transfer is necessary to conclude the contract; or
- the transfer is necessary to carry out such a contract.

In this context, contracts are not restricted to goods and services. They can include employment contracts. Deciding whether a transfer is necessary to carry out a contract depends on the nature of the goods or services provided under the contract rather than how the MPS is organised.

A transfer cannot be considered necessary if the only reason the MPS needs to make it is because of the way in which the MPS has chosen to structure the organisation; i.e. In the unlikely circumstances that the MPS moves all of its HR functions to a third country, the transfer of personal data will not be considered necessary under the Act just because of this re-organisation in structure.

8.3.2 Substantial Public Interest

The MPS can transfer personal data overseas where it is necessary for reasons of substantial public interest. This is a high threshold to meet, however, the prevention and detection of crime and National Security purposes are covered by this exemption. When applying this exemption, Business Groups must be able to demonstrate that the decisions made were on a strict case-by-case basis and that there is significant public interest reasons

to proceed with the transfer. Business Groups must note that the public interest grounds must be that of the UK and not of the 'third country' to which the personal data is transferred.

8.3.3 Vital Interests

The MPS can transfer personal data overseas where it is necessary to protect the vital interests of an individual or individuals. This relates **only** to matters of life and death.

8.3.4 Legal Claims

The MPS can transfer personal data overseas where it is necessary:

- in connection with any legal proceedings, including future proceedings not yet underway;
- to get legal advice; or
- to establish, exercise or defend legal rights.

The legal proceedings do not have to involve the MPS or the individual as a party and the legal rights do not have to be the MPS or the individual's. Although this exemption could apply widely, transfers are only likely to fall under this category if they are connected with legal proceedings or obtaining legal advice.

8.3.5 National Security (Section 28)

Personal data are exempt from the requirements to meet any of the Data Protection Principles, including the 7th and 8th principle, where the processing is for the purpose of safeguarding national security. However, the application of this exemption may require a National Security Certificate signed by the Home Secretary. For further advice refer to the Data Protection Officer or the Deputy Data Protection Officer.

9. Refusal of Authority to Transfer

<u>In circumstances where none of the available transfer options discussed in these SOPs are suitable for the intended processing, the processing will not meet the legal requirements of the Act and will not be approved to proceed.</u>

Further guidance on the application of this SOP and project or case specific guidance can be obtained from the Data Protection Officer or the Deputy Data Protection Officer.

10 SECURITY REQUIREMENTS FOR INTERNATIONAL DATA TRANSFERS

Once you are satisfied that the international data processing satisfies the 8th Data Protection Principle (Sections 6 - 8 above), there is also a requirement to meet the 7th Data Protection Principle regarding the security of the personal data.

Principle 7 *- Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.*

The seventh principle (extract from the text of the Act)

9 - Having regard to the state of technological development and the cost of implementing any measures, the measures must ensure a level of security appropriate to -

(a) the harm that might result from such unauthorised or unlawful processing or accidental loss, destruction or damage as are mentioned in the seventh principle, and

(b) the nature of the data to be protected.

10 - The data controller must take reasonable steps to ensure the reliability of any employees of his who have access to the personal data.

11 - Where processing of personal data is carried out by a data processor on behalf of a data controller; the data controller must in order to comply with the seventh principle -

(a) choose a data processor providing sufficient guarantees in respect of the technical and organisational security measures governing the processing to be carried out, and

(b) take reasonable steps to ensure compliance with those measures.

12 - Where processing of personal data is carried out by a data processor on behalf of a data controller; the data controller is not to be regarded as complying with the seventh principle unless -

(a) the processing is carried out under a contract -

(i) which is made or evidenced in writing, and

(ii) under which the data processor is to act only on instructions from the data controller, and

(b) the contract requires the data processor to comply with obligations equivalent to those imposed on a data controller by the seventh principle.

Secure Transfer

The 7th Data Protection Principle requires that personal data is appropriately protected. Personal data, unless it is otherwise publicly available, will normally attract a minimum protective marking of PROTECT. Personal data detailing intelligence and or conviction details will usually attract a higher protective marking. If you intend to transport personal data overseas using a portable device it **must** be encrypted. See METSEC Code (MPS Security Manual) **METSEC Code TEC 9.3** for further details.

The import and export of cryptographic technology is subject to international agreements and individual laws relating to the country concerned. Many mobile computer devices, such as laptops, now incorporate encrypted hardware or software and computer equipment maybe scanned for such cryptography at airports etc. when entering certain countries. Cryptographic Technology usually refers, in simple terms, to the technical means to render information unintelligible by encryption (i.e. by encoding or 'scrambling') often prior to transfer of the information, so that it cannot be read 'in clear' if intercepted in transit. A high level of security is usually characteristic of encryption but in spite of the complexity involved any encryption applied is at least in theory capable of being 'cracked'. There could also exist latent weaknesses in technical or management processes that could be vulnerable to exploitation by a determined computer 'hacker'. Encrypted information is designed to be decrypted (i.e. by decoding or 'unscrambing') and at a later date read by authorised persons when it is restored to a clear, legible form usually following transmission.

Within the European Community (EC) you may move cryptographic technology freely across all international EC borders and use it in all EC Countries. See **METSEC Code TEC 9.4**. If you intend to transport cryptographic technology outside of the EC you must contact the Information Assurance Unit by email to 'DoI Mailbox - Security Advice' or telephone to 785084 for appropriate advice.

If it is intended to use the Internet to transmit the personal data, RESTRICTED information may only be sent via the Internet if it is encrypted using CESG approved products (see **METSEC Code TEC 2.3.6)**. Information attracting a protective marking of CONFIDENTIAL, SECRET or TOP SECRET **must** not be transmitted via the Internet. Advice on encryption of documents can also be obtained from the Information Assurance Unit.

Security Assurance

If overseas transfer of personal data is to take place as part of an established information sharing arrangement, or as part of an offshoring exercise the Information Security Officer

(ISO) must be consulted from the outset. The ISO will need to discuss the provision of specialist advice and guidance covering the personnel, physical and technical security risks associated with the initiative. It is expected that systems procurement, projects, contracts and other initiatives make available sufficient resources to ensure secure methods for transferring personal data abroad. This will apply whether or not the service is out-sourced or not. Systems involving international transfer of personal data will also be subject to requirements for security accreditation and assurance. Advice can be obtained from the ISO.

11. RESPONSIBILITIES

Ownership of SOPs:	Enterprise Architecture Board (EAB)
Implementing SOPs:	DoI2 (3-3) Public Access Office (PAO)
Compliance with SOPs:	DoI2 (3-3) Public Access Office (PAO)
Reviewing SOPs:	DoI2 (3-1) Information Assurance Unit (IAU)

12. ASSOCIATED DOCUMENTS & POLICIES

12.1 Documents Replaced

None

12.2 Associated and Linked Reference Documents

- MPS Information Management Policy.
- Data Protection Act 1998 (DPA) Compliance SOPs
- ACPO Media Guidance on the Release of Images of Suspects and Defendants
- ACPO and CPS on Publicity and the Criminal Justice System
- Home Office Guidelines on the Publishing of ASBOs

These SOPs have been developed from and adhere to the ACPO Data Protection Manual of Guidance and the Information Commissioner's Office (ICO) ICO’s specialist guidance on international data transfers.

12.3 Relevant Legislation

- Data Protection Act 1998 (DPA)
- European Data Protection Directive 95/46/EC

- Human Rights Act 1998 (HRA)
- Coroners & Justice Act 2009 c.25

13. ABBREVIATIONS & DEFINITIONS

13.1 Abbreviations

ACRO	Association of Chief Police Officers Criminal Records Office
CMS	Content Management System
CRIMINT	Crime Intelligence System
CRIS	Crime Recording & Information System
CTC	Counter-Terrorism Command
DPA (or 'The Act')	Data Protection Act 1998
DLS	Directorate of Legal Services
DPO	Data Protection Officer
DDPO	Deputy Data Protection Officer
EEA	European Economic Area
EU	European Union
HRA	Human Rights Act 1998
IAU	Information Assurance Unit [or International Assistance Unit]
ICO	Information Commissioner's Office
ISO	Information Security Officer
IIEE	TP Emerald - International Intelligence & Evidence Exchange
METSEC Code	The MPS Security Code Manual
MPA	Metropolitan Police Authority
MPS	Metropolitan Police Service
PAO	Public Access Office
SOCA	Serious Organised Crime Agency
SOPs	Standard Operating Procedures
UKCA-ECR	UK Central Authority for the Exchange of Criminal Records

14. CONTACTS & SUGGESTED AMENDMENTS

14.1 Contacts

Data Protection Officer (DPO)

Deputy Data Protection Officer (DDPO)

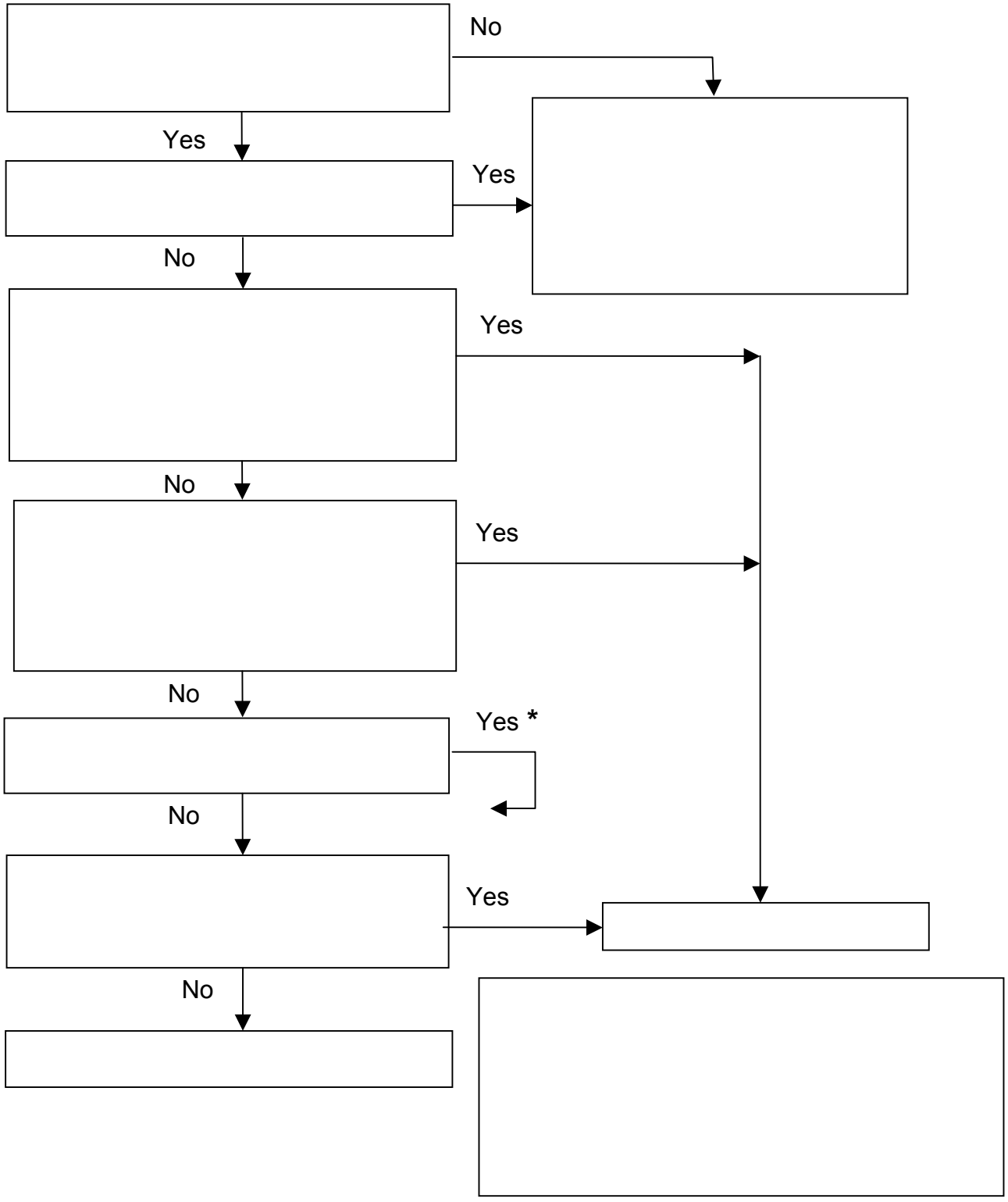
Information Security Officer (ISO)

14.2 Amendments

Any suggested amendments to inform future SOPs, or highlighting any spelling or grammatical errors within this document can be communicated either using the corporate policy Feedback Form found on the Corporate Policy Database; by email to 'DoI Mailbox - Security Advice' or in writing via despatch to Information Assurance Unit (IAU), DoI2 (3-1), Floor 1 West, Edinburgh House. Any suggestions will be noted for consideration to change the SOPs as deemed appropriate at the next review.

Appendix A - Lawfully Transferring Personal Data Internationally

Can I Send Personal Data Abroad? A Quick Reference Flow Chart.



Appendix B - General Adequacy Assessment Grid

	RISK			Risk Mitigation Proposals	Balanced Risk			Relevant Information
	High	Medium	Low		High	Medium	Low	
Does the data fall under the definition of 'Sensitive Personal Data'?	Yes	No	No		Yes	No	No	
Is the processing in line with our 'registered purposes?'	No	NA	Yes					If the answer is no then the processing cannot proceed. Contact the Data Protection Officer for further advice.
Will the data be processed internationally for more than 2 months?	Yes	NA	No					If the data is only going to be processed once or for a short time and then destroyed, then the risks arising from any lack of protection may be less than if the data is being processed on a long-term basis.
Does the transfer meet MPS security requirements, including risk assessment, counter-measures and procedures?	No	NA	Yes		No	NA	Yes	If the transfer does not meet these basic security standards permission to proceed is unlikely to be granted. If this is the case please seek the advice of the Information Security Officer (ISO)
Does the data originate from the EEA or	Yes	NA	No	(If the answer is yes, there will be a requirement to				If the originating country was a third country the protection of the EU directive and the DPA is not intended to provide an extended level of protection

'safe country'?				ensure all requirements of the DPA are met)				to the citizens of that third country beyond that what is provided by the country's own legislative protection [if any]. If the data originates from the EEA or 'safe country' there will be a level of expectation that the data will be processed inline with the requirements of the DPA.
Will the final destination of the transfer be within the EEA or 'safe country'?	No	NA	Yes					In some cases it is known that there will be a further transfer to another country or territory which may or may not be outside the EEA. If this is the case, then the protection given in that ultimate destination will be relevant in assessing adequacy.

Note: 'Sensitive Personal Data' means personal data consisting of information as to:

(a) the racial or ethnic origin of the data subject,
(b) his political opinions,
(c) his religious beliefs or other beliefs of a similar nature,
(d) whether he is a member of a trade union [within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992],
(e) his physical or mental health or condition,
(f) his sexual life,
(g) the commission or alleged commission by him of any offence, or
(h) any proceedings for any offence committed or alleged to have been committed by him, the disposal of such proceedings or the sentence of any court in such proceedings.