INTERPOL

ECOWAS

WAPIS GUIDE

BEST PRACTICE GUIDE ON PERSONAL DATA PROTECTION

JUNE 2020

This Project is funded by the European Union

The West African Police Information System Best Practice Guide on Personal Data Protection has been drafted by the WAPIS Programme Team under the auspices of INTERPOL's Office of Legal Affairs and with the invaluable contributions of Teki Akuetteh and Dr Mouhamadou Lo, both of whom are experts in the field of data protection.

This Programme is funded by the European Union

DISCLAIMER

The content of this brochure does not reflect the official opinion of the European Union. Responsibility for the information and views expressed in the document lies entirely with the author(s).

GENERAL FRANCIS
A. BEHANZIN
ECOWAS Commissioner for
Political Affairs, Peace and
Security

PREFACE

In seeking to take an important step, through the sharing of criminal intelligence, to better manage the fight against organized crime in general, and terrorism in particular, in West Africa, the ICPO-INTERPOL should be congratulated. With almost 100 years of experience (1923-2020) in the field of police investigations, the Organization has brought the 15 Member States of ECOWAS and Mauritania the EU-funded West African Police Information System (WAPIS). The WAPIS Programme was originally developed to facilitate the detection of criminal offences, the collection of evidence relating to offences and the search for possible perpetrators and accomplices, with a view to combating transnational crime and terrorism, and has in turn led to the processing of personal data and also provides for data concerning witnesses and victims to be recorded if that is required by the investigation. As part of this important ECOWAS project, law enforcement agencies (Police, Gendarmerie, Customs, Immigration, Water, Forestry and assimilated services) will be sharing sensitive information on both people and property with the ultimate goal of securing people and property in the ECOWAS area, the African continent as a whole, Europe and throughout the world. These agencies will be sharing personal data, i.e. any information relating to an individual who has been identified or who may be directly or indirectly identifiable through an identification number or one or several unique identifying features.

Such data are protected in West Africa by Supplementary Act A/SA.1/01/10 on Personal Data Protection within ECOWAS, which was adopted on 16 February 2010, to protect citizens in the Community from abuse in the collection and processing of such personal data. The Supplementary Act therefore established the basic principles applicable to the processing of personal data and directed ECOWAS Member States to enact data protection legislation and to establish adequate data protection authorities with responsibility for enforcing the right to personal data protection.

WHY SHOULD PERSONAL DATA BE PROTECTED?

Protecting personal data is about protecting privacy, dignity and other fundamental human rights such as the right to privacy, image rights, the right to honour, etc.

It is in this context, and with the aim of assisting law enforcement in processing personal data in WAPIS in conformity with the Supplementary Act, other applicable laws and regulations in the countries concerned, as well as international data protection standards, that this Best Practice Guide on Personal Data Protection has been put together.

This Guide was drafted by the WAPIS Programme and approved by the representatives of the countries taking part in the Programme during the ECOWAS Expert Committee Meeting to harmonize legislation held in Abidjan, from 22 to 24 October 2019. It is based on national and international best practices in accordance with the ECOWAS Supplementary Act and the laws in force in the countries participating in the Programme. This Best Practice Guide, although not binding, is intended to provide guidance to facilitate understanding of established standards and guidelines for the collection, processing, sharing, use and retention of personal data under the WAPIS Programme.

By adhering to this Guide, law enforcement authorities will enable countries taking part in the Programme to adopt best practices that will facilitate information sharing and maximize the use of WAPIS while striking the necessary balance between effective law enforcement and respect for every individual's recognized fundamental rights and freedoms.

I call on the countries participating in WAPIS to take full advantage of this Guide to maximize their capacity to combat transnational crime and terrorism through the sharing of quality information.

General Francis A. BEHANZIN
Commissioner for Political Affairs, Peace and Security

CONTENTS

INTRODUCTION 6

› What is the WAPIS Best Practice Guide on Personal Data Protection? 6

› The purpose of the WAPIS BPG 6

› Overview of the WAPIS BPG 8

CHAPTER I - GENERAL TERMINOLOGY 11

CHAPTER II - APPLICABLE PRINCIPLES OF PERSONAL DATA PROTECTION AND PURPOSE OF PROCESSING 13

› 2.1 Applicable Principles 13

› 2.2 Purpose of processing data in the System 15

CHAPTER III - DATA PROTECTION REGIME AND GOVERNANCE 17

› 3.1 Control and notification 17

› 3.2 Data Protection Officer (DPO) and Data Protection Awareness and Training 18

› 3.3 Data Protection Compliance and Governance 20

CHAPTER IV - PERSONAL DATA COLLECTION AND SHARING 25

› 4.1 Collection of Personal Data 25

› 4.2 Sharing or Transmission of data to other public bodies 27

› 4.3 Sharing or Transmission of data to other public bodies 28

› 4.4 Sharing or Transmission of data internationally 31

CHAPTER V - DATA QUALITY, CONFIDENTIALITY AND SECURITY 32

› 5.1 Data Quality 32

› 5.2 Confidentiality and Security 34

CHAPTER VI - DATA BREACHES 37

› 6.1 Data breach notification 37

› 6.2 Data Breach Notification to Data Subject 37

CHAPTER VII - PROCESSING RECORDS AND DATA RETENTION 41

› 7.1 Records of processing activities 41

› 7.2 Logs 41

› 7.3 Data retention 42

CHAPTER VIII - SENSITIVE DATA PROCESSING 44

› 8.1 Sensitive Data processing 44

CHAPTER IX - DATA SUBJECT RIGHTS 46

› 9.1 Right to access 46

› 9.2 Right to rectification or erasure 49

CHAPTER X - DATA PROTECTION IMPACT ASSESSMENT 51

› 10.1 Data Protection Impact Assessment 51

CHAPTER XI - EXCEPTIONS 53

› 11.1 Exceptions from the processing of data in accordance with this guide 53

CHAPTER XII - CONCLUSION 54

KEY TAKEAWAYS 55

INTRODUCTION

WHAT IS THE WAPIS BEST PRACTICE GUIDE ON PERSONAL DATA PROTECTION?

The purpose of this West African Police information System ('WAPIS' or 'the System') Best Practice Guide ('BPG') on Personal Data Protection is to assist law enforcement authorities in processing data in the WAPIS in conformity with the 'Supplementary Act A/SA.1/01/10 on Personal Data Protection within ECOWAS' ('Supplementary Act'), other applicable laws and regulations as well as international standards and best practice on personal data processing.

The BPG is intended for all law enforcement authorities and entities that process personal data through the System. It provides guidance on data protection for the processing of personal data in the System. It aims to facilitate understanding of existing laws and law enforcement guidelines applicable to the processing of data by law enforcement authorities in the WAPIS participating countries.

The WAPIS BPG does not absolve ECOWAS Member States from their obligations under the Supplementary Act, notably the obligation to adopt national data protection legislation and establish a data protection authority.

The WAPIS BPG is a data protection guidance tool expressly developed for the WAPIS participating countries to ensure best practices are applied in the collection, processing, sharing and use of personal data in the System. It represents a benchmark for national and international best practice in accordance with the ECOWAS Supplementary Act and those beneficiary countries that have data protection laws. It defines the core data protection principles, exemptions and rights while incorporating governance and compliance structures to facilitate implementation.

THE PURPOSE OF THE WAPIS BPG

The WAPIS is an electronic police information system that operates on a national, regional and international level. Its overall objective is to increase the capacity of West African law enforcement authorities to combat transnational crime and terrorism through enhanced information management and sharing. The System contains law enforcement information, including, but not limited to, information concerning:

a. People (such as suspects, witnesses and victims);
b. Modes of transport (such as cars);
c. Documents (such as passports, driving licences, national ID cards, etc.);
d. Weapons;
e. Locations;

f. Events; and
g. Generic items (this may include objects not falling within the defined categories - e.g. certain items found on a crime scene).

Some of these data come under the definition of 'personal data', in that they could lead – directly or indirectly – to the identification of an individual.

At regional level, the ECOWAS High Contracting Parties, aware of the potentially detrimental impact that the processing of personal data could have on the fundamental rights and freedoms of data subjects, adopted the Supplementary Act on 16 February 2010. The Supplementary Act lays down the fundamental principles applicable to the processing of personal data within ECOWAS and requires its member countries to enact data protection legislation and establish data protection authorities. WAPIS participating countries are currently at different stages of compliance with these key requirements.

The BPG is a response to a request made during the WAPIS Legal Seminar held on 19 March 2019, convened by the ECOWAS Commission, INTERPOL and the European Union, and attended by WAPIS focal points and legal experts from 16 WAPIS participating countries. In the light of the concerns that were raised about the lack of data protection legislation and non-existence of data protection authorities in some WAPIS participating countries, it was proposed that a draft 'best practice' guide concerning the processing of personal data in the WAPIS System be presented to the WAPIS focal points and legal experts during a dedicated legal workshop, for their consideration. The draft BPG was presented at a follow-up legal seminar, also convened by the ECOWAS Commission, INTERPOL and the European Union, that took place in Abidjan from 22 to 24 October 2019, and was endorsed by the participants.

OVERVIEW OF THE WAPIS BPG

This Guide is divided into 12 chapters.

The first chapter provides an overview of terminology used in the Guide. Notably, it defines terminology relating to the key entities bearing responsibility for personal data protection under the Guide (Ch. 1, paras. 1, 2), recipients of personal data (Ch. 1, para. 8), individuals whose personal data are subject to processing, (Ch. 1, para. 4), and the type of information that constitutes personal data (Ch. 1, para. 7).

The second chapter presents general personal data protection principles and legitimate law enforcement reasons for processing data. The personal data protection principles provide law enforcement authorities with a general understanding of the various requirements for processing personal data in the WAPIS. The personal data protection principles described relate to: (a) consent and legitimacy; (b) legality and fairness; (c) purpose, relevance and preservation; (d) accuracy; (e) transparency; (f) confidentiality and security; and (g) choice of data processor. Law enforcement authorities should only process data in the WAPIS for legitimate law enforcement purposes, which include: the prevention, investigation, detection or prosecution of an offence, the execution of penalties, the maintenance of public order, safeguarding against and preventing threats to public security, or any duty or responsibility of law enforcement authorities arising from law.

The third chapter discusses the role of data protection authorities, the significance of data protection training, and the importance of engaging key stakeholders to implement the data protection framework. First, all WAPIS participating countries should establish an independent data protection authority responsible for data processing operations. Second, law enforcement authorities should designate a Data Protection Officer to: (a) advise law enforcement authorities of legal obligations; (b) monitor compliance; (c) provide advice concerning data protection impact assessments; (d) liaise with data protection authorities; and (e) dispense suitable ongoing training to WAPIS users. Third, law enforcement authorities should incorporate data protection into their governance structures by engaging key stakeholders in the WAPIS data protection framework.

The fourth chapter lays out best practices for the collection and sharing of personal data. As a general rule, the collection of personal data should be limited to what is strictly necessary and proportionate to the purpose for which the personal data is collected.

The fifth chapter provides an overview of data quality and measures that law enforcement authorities should implement to ensure personal data remains confidential and secure. As a general rule, law enforcement authorities should not share inaccurate, outdated or incomplete personal data. If law enforcement authorities realise they have disclosed inaccurate personal data, they should notify the recipient without delay and take appropriate steps to rectify or erase the data and restrict data processing. Furthermore, law enforcement authorities should take appropriate measures to secure the System.

The sixth chapter specifies the appropriate steps to take in the event of a data breach. Law enforcement authorities should document and report a data breach to the appropriate data protection authority without undue delay, preferably within seventy-two hours of the initial breach. Furthermore, law enforcement authorities should notify data subjects of a data breach without undue delay if the breach is likely to pose a risk to the rights and freedoms of the person in question.

The seventh chapter outlines best practices for processing records and data retention. Law enforcement authorities should keep records of all data processing activities. In addition, law enforcement authorities should keep logs of data regarding (a) collection; (b) alteration; (c) access/consultation; (d) disclosure, including transfers; (e) combination; and (f) erasure. Furthermore, law enforcement authorities should only retain data for an appropriate period of time.

The eighth chapter explains that sensitive data ["Personal data revealing the racial, ethnic or regional origin, parentage, political opinions, religious or philosophical beliefs, trade union membership, sexual life, genetic data or more generally data on the state of health of an individual" (Ch. 8.1, para. 1)] should not be processed in the WAPIS, except when strictly necessary.

The ninth chapter highlights data subjects' rights, namely the right to access, rectify or erase data. The right of access allows a data subject to have direct or indirect access to personal data pertaining to them in the WAPIS, while the right of rectification or erasure allows a data subject to request law enforcement authorities to rectify or erase inaccurate personal data relating to them in the WAPIS.

The tenth chapter discusses the data protection impact assessment, a process that can be used to help law enforcement authorities assess and record risks involved in processing personal data in the System. A properly executed data protection assessment will evidence that law enforcement authorities considered the risks related to the intended data processing.

The eleventh chapter lists the situations where data should not be processed in accordance with this Guide.

The twelfth chapter summarizes the overall purpose of this Guide, which is to enable WAPIS participating countries to engage in lawful data processing practices that facilitate information management and sharing and maximize overall use of WAPIS.

CHAPTER I

GENERAL TERMINOLOGY

For the purposes of this guide:

1. 'Data controller' means any public or private individual or legal entity, body or association who, alone or jointly with others, decides to collect and process personal data and determines the purposes for which such data are processed.[1]
2. 'Data processor' means any public or private individual or legal entity, body or association who processes data on behalf of the data controller.[2]
3. 'Data protection authority' means an independent body responsible for data protection compliance, established by a WAPIS participating country in accordance with Article 14 of the Supplementary Act and/or local laws in the participating country.
4. 'Data subject' means an individual who is the subject of personal data processing.[3]
5. 'Personal data breach' means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed.[4]
6. 'Personal data processing' means any operation or set of operations performed on personal data whether or not by automated means such as obtaining, using, recording, organizing, preserving, adapting, altering, retrieving, saving, copying, consulting, utilizing, disclosing by transmission, disseminating or otherwise making available, aligning or combining, as well as blocking, encrypting, erasing or destroying such data.[5]
7. 'Personal data' means any information relating to an identified individual who may be directly or indirectly identifiable by reference to an identification number or one or several elements related to their physical, physiological, genetic, psychological, cultural, social, or economic identity.[6]
8. 'Recipient' means a natural or legal person, public authority, agency or other body, to which the personal data are disclosed, whether or not it be a third party.[7]

1 Supplementary Act A/SA.1/01/10 on Personal Data Protection within ECOWAS, 16 February 2010, Article 1.

2 Supplementary Act A/SA.1/01/10 on Personal Data Protection within ECOWAS, 16 February 2010, Article 1.

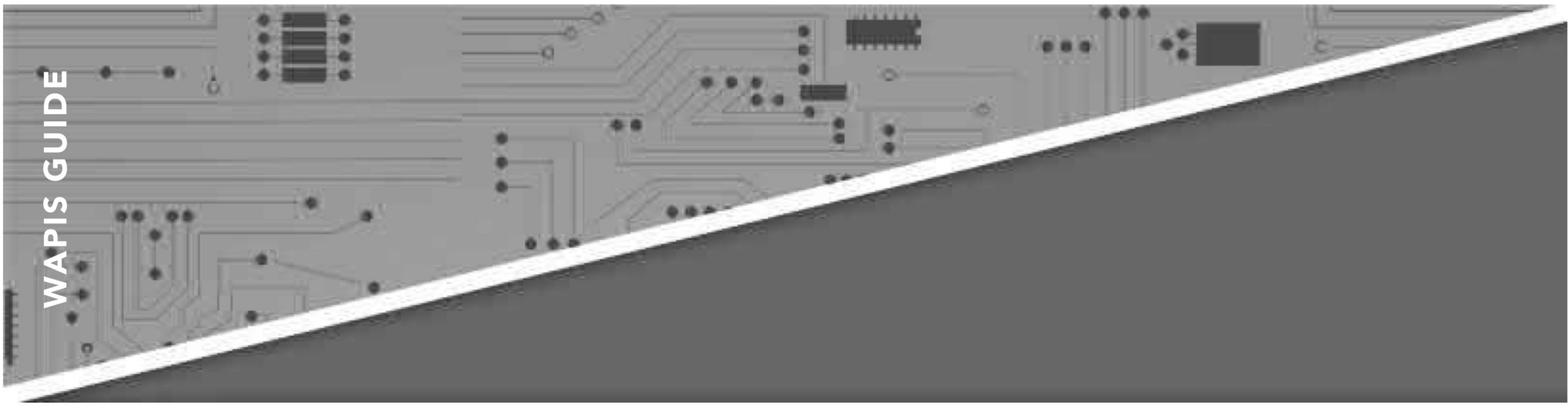
3 Supplementary Act A/SA.1/01/10 on Personal Data Protection within ECOWAS, 16 February 2010, Article 1.

4 Directive (EU) 2016/680, 27 April 2016, Art. 3(11).

5 Supplementary Act A/SA.1/01/10 on Personal Data Protection within ECOWAS, 16 February 2010, Article 1.

6 Supplementary Act A/SA.1/01/10 on Personal Data Protection within ECOWAS, 16 February 2010, Article 1.

7 Directive (EU) 2016/680, 27 April 2016, Art. 3(10).



9. 'Sensitive Data' means personal data relating to an individual's religious, philosophical, political or trade union opinions or activities, to an individual's sexual life, racial origin or health, relating to social measures, proceedings and criminal or administrative sanctions.[8]
10. 'Supplementary Act' means the ECOWAS Supplementary Act A/SA.1/01/10 on Personal Data Protection of 16 February 2010.
11. 'WAPIS participating country' refers to any of the following countries: Republic of Benin, Burkina Faso, Republic of Cabo Verde, Republic of Chad, Republic of Côte d'Ivoire, Republic of The Gambia, Republic of Ghana, Republic of Guinea, Republic of Guinea-Bissau, Republic of Liberia, Republic of Mali, Islamic Republic of Mauritania, Republic of Niger, Federal Republic of Nigeria, Republic of Senegal, Republic of Sierra Leone or the Togolese Republic.
12. 'WAPIS' (or the 'System') means the West African Police Information System - an electronic police information system that will operate on a national, regional and international level.

8 Supplementary Act A/SA.1/01/10 on Personal Data Protection within ECOWAS, 16 February 2010, Article 1.

CHAPTER II

APPLICABLE PRINCIPLES OF PERSONAL DATA PROTECTION AND PURPOSE OF PROCESSING

2.1 APPLICABLE PRINCIPLES

When processing personal data in the System, law enforcement authorities should be guided by the following principles, set out in Chapter V of the Supplementary Act:

1. The principle of consent and legitimacy: Law enforcement authorities should process personal data for legitimate reasons, notably ensuring that such processing is necessary, inter alia:
   a. To comply with a legal obligation that is binding on a law enforcement authority;
   b. For the implementation of a public interest or other relevant mission necessary in the exercise of public authority that is vested in the law enforcement authority.

   Data processing for the law enforcement purposes set out in paragraph 2.2 below is exempted from the obligation to obtain consent of the data subject.
2. The principle of legality and fairness: Law enforcement authorities should process personal data in a legal, fair and non-fraudulent manner. All processing should be authorized by law and must respect the basic rights of data subjects, in accordance with the applicable human rights obligations. The main purpose is to protect the interests of the individuals whose personal data are being processed. It covers all handling of personal data in the System. It is important to understand that it is not because the processing of the personal data of an individual has a negative effect on the individual that it is automatically unfair, unreasonable or unlawful. The decision is based on whether the negative effect is legally justifiable for detection, prevention or other law enforcement purposes. In practice, this means that the law enforcement authorities should:
   a. Have legitimate grounds for collecting, using and processing personal data in the System;
   b. Refrain from using the information or data in ways that have unjustifiable adverse effects on the individuals concerned;
   c. Be transparent about how they intend to use the data, and provide appropriate data protection notices;
   d. Handle or process the personal data only as reasonably expected under the System; and

e. Make sure the users of the System do not make unlawful use of the personal data.

3. Principle of purpose, relevance and preservation: Law enforcement authorities should collect personal data for specified, explicit, and lawful purposes and should ensure that such data are not further processed in any manner incompatible with such purposes. The personal data should be adequate and relevant in relation to the purposes for which it is collected and subsequently processed. The personal data should only be retained for the requisite period for the purposes for which they were obtained or processed. Beyond the required period, data should only be kept for historical, statistical, and research purposes, in line with existing legal provisions.
4. Principle of accuracy: Law enforcement authorities should ensure that the personal data obtained are accurate and, where necessary, kept up-to-date. All reasonable measures should be taken to ensure that data that is inaccurate and incomplete with regard to the purposes for which it was obtained and processed is erased or rectified.
5. Principle of transparency: Law enforcement authorities should provide information about the processing of personal data, subject to applicable exceptions.
6. Principle of confidentiality and security: Law enforcement authorities should ensure that data in the system is processed confidentially and that it is protected. The level of confidentiality of data processed in the System should be determined according to the risks linked to their disclosure for data subjects as well as the sources.
7. Principle of choice of data processor: Where processing is carried out on behalf of law enforcement authorities, said law enforcement authorities have an obligation to choose a data processor providing sufficient guarantees. It is the responsibility of the law enforcement authorities as well as the data processor to ensure compliance with the applicable data protection principles.

CHAPTER II

1. Do not illegally collect personal data
2. Respect the fundamental rights of the data subjects, notably human rights
3. Do not process personal data in an unfair, unreasonable or unlawful manner
4. Ensure that any processing of data has a specific, explicit and legitimate purpose
5. Set and manage retention periods for personal data
6. Ensure that the personal data collected is accurate and, if necessary, kept up-to-date
7. Erase or rectify inaccurate or incomplete data
8. Manage personal data in a transparent manner
9. Secure the System and ensure the confidentiality of personal data
10. Supervise subcontractors working in the System

2.2 PURPOSE OF PROCESSING DATA IN THE SYSTEM

1. The processing of data in the System should be restricted to one or more of the following law enforcement purposes:
   - **a.** Prevention of offences;
   - **b.** Investigation of offences;
   - **c.** Detection of offences;
   - **d.** Prosecution of offences;
   - **e.** Execution of penalties;
   - **f.** Maintaining public order;
   - **g.** Safeguarding against, and preventing, threats to public security; and
   - **h.** Any duty or responsibility of law enforcement authorities arising from law.

2. Personal data collected for law enforcement purposes should not be used for any other purpose that is incompatible with the original law enforcement purpose for which they were collected, unless permitted by law.

BEST PRACTICE

PURPOSE OF PROCESSING DATA

1. Adhere to the stated purposes of processing data in the System

2. Before expanding the scope of the processing purposes, ensure that it is legal to do so

3. Do not pervert the stated processing purposes

CHAPTER III

DATA PROTECTION REGIME AND GOVERNANCE

3.1 CONTROL AND NOTIFICATION

1. Each WAPIS participating country should have an independent data protection authority, in accordance with Article 14 of the Supplementary Act.

2. The System should be declared to the data protection authority in accordance with the laws of the WAPIS participating country.

3. Where the WAPIS participating country is yet to adopt laws or set up the requisite independent data protection authority, it should publish the Supplementary Act in its Official Journal and respect the principles set out in the Act. It could also set up or designate an independent oversight body to perform the functions of the data protection authority.

4. Each WAPIS participating country should put in place legal frameworks, in the form of laws, regulations, rules, directives, policies etc., that clearly identify the law enforcement authorities responsible for the processing of data in the System and specify how personal data is to be processed in the System.

5. A law enforcement authority is responsible for all data processing that it undertakes, or permits to be undertaken, and is accountable for such data processing operations.

BEST PRACTICE

CONTROL AND NOTIFICATION

1. Put in place a personal data protection law and establish an independent personal data protection authority in accordance with Article 14 of the Supplementary Act.

2. Declare the System to the data protection authority.

3. Raise awareness among public authorities that have not yet adopted data protection legislation on the urgency of publishing the Supplementary Act in their official journal.

3.2 DATA PROTECTION OFFICER (DPO) AND DATA PROTECTION AWARENESS AND TRAINING

1. Law enforcement authorities should appoint a data protection officer possessing a sound understanding of data protection law and practice in order to perform the following tasks:
   a. Inform and advise the law enforcement authorities processing data in the System of their legal obligations regarding the processing of personal data;
   b. Monitor compliance of the law enforcement authorities with regard to the processing of data in the System;
   c. Provide advice where requested concerning data protection impact assessments;
   d. Cooperate and liaise with the relevant data protection authorities; and
   e. Implement suitable ongoing training programmes in data protection for persons working on the System.
2. Where applicable, appropriate certification and training should be mandatory for the DPO.
3. Law enforcement authorities participating in the WAPIS Programme should ensure that data protection awareness and training is given to all users of the System.
4. The data protection officer should be adequately trained and/or certified to manage the WAPIS data protection framework.

BEST PRACTICE

DATA PROTECTION OFFICER

1. Appoint a data protection officer

2. Ensure that the data protection officer has the right profile for the job

3. Establish a capacity building programme on data protection for the data protection officer and users of the System

ON DATA PROTECTION TRAINING FOR LAW ENFORCEMENT AUTHORITIES

Dyfed Powys Police, ICO Undertaking, Ref. COM0666484, COM0672404, COM0677576

After an audit, the Information Commissioner's Office (ICO), the United Kingdom's Data Protection Authority, ascertained that 1,204 of the 2,258 officers had not undergone data protection training resulting in numerous violations of the Data Protection Act. These included an officer faxing sensitive data on an open fax machine without the individual's permission and another distributing a photograph of their desk which included an image of his computer screen displaying personal and sensitive data. The Information Commissioner mandated the following:

- Establishment of a force-wide programme of data protection training
- Establishment of a force-wide programme of refresher training to ensure ongoing compliance with the Data Protection Act
- A programme of recording and monitoring of training programmes
- Any other security measures as are appropriate to ensure that personal data is protected against unauthorized and unlawful processing, accidental loss, destruction, and/or damage.

Humberside Police, ICO Undertaking, Ref. COM06493155

In response to an incident concerning the loss of unencrypted disks containing an interview with an alleged rape victim, the Humberside Police was audited by the Data Protection Authority. The audit concluded that the department was only 16.8% compliant in relation to data protection training. The Data Controller took the necessary measures to ensure:

- All current staff members responsible for handling personal data receive appropriate, specific data protection training within six months;
- All staff members who regularly handle removable media such as CDs, DVDs, and USB memory sticks receive training about the use of encryption, including when it is appropriate and how to encrypt;
- Annual refresher training programmes are conducted;
- New staff members responsible for handling personal data are given appropriate, specific data protection training upon induction;
- Training programme compliance is monitored;
- The Data Protection Authority's policies and procedures are promoted and made available to staff in all departments that handle personal data.

3.3 DATA PROTECTION COMPLIANCE AND GOVERNANCE

1. To ensure compliance with data protection principles in the implementation and operation of the WAPIS, law enforcement authorities should process all personal data in such a way as to minimise risks associated with unauthorized and unlawful processing of such data.
2. Law enforcement authorities should incorporate privacy and data protection into their governance structures to align the requirements of data protection principles with their organisational goals and culture. This can be achieved by understanding the data protection principles, their scope, identifying organisation-wide compliance gaps, creating plans to close those gaps and strategically implementing the plans, policies and procedures.
3. Law enforcement authorities should also implement policies that ensure staff or employees are assigned clear responsibilities for data protection and are held accountable for their actions.
4. Strategic governance interventions that can facilitate implementation of the principles include the following:
   a. Assign responsibility for data protection matters in the implementation and operation of the WAPIS to a specific individual – such as the Data Protection Officer (DPO). The DPO should be responsible for facilitating compliance within the WAPIS. The DPO should handle the day-to-day data protection management of the WAPIS. The DPO may occupy a designated data protection role and/or be part of the legal, compliance, IT, security or information management departments.
   b. Raise awareness and involve high-level administrators in the management of the data protection framework for WAPIS. The implementation of a data protection framework requires senior management involvement to facilitate smooth implementation. Such support may include:
      i. Communicating on the importance of data protection within the System to all staff and subordinate management;
      ii. Participating in data protection initiatives; and
      iii. Providing adequate funding to support data protection activities.
   c. Assign responsibility for the WAPIS data protection framework across the law enforcement authority. Managing data protection will require the contribution and participation of almost all WAPIS users. The DPO may therefore set up a data protection team to work in the different functional groups within the unit to facilitate understanding of the data protection risks applicable to that functional group.

d. Ensure regular communication between the DPO and the data protection team and those responsible for data protection within WAPIS. This may help effectively implement the data protection framework in order to:
   i. Proactively assist in building data protection into ongoing projects; and
   ii. Help users meet their objectives.

e. Engage all key stakeholders in the WAPIS data protection framework. The DPO should communicate with System users. Key stakeholder engagements may take the form of formal discussions or meetings (e.g. monthly or quarterly meetings) on the WAPIS data protection framework. The DPO should also be involved in activities that may impact data protection such as information security, investigations and intelligence gathering, etc.

f. Report to internal officials such as senior management on the status of the data protection framework in a regular and consistent manner. Such reports should highlight major data protection risks, data breaches or events, etc. Timely and accurate reporting on privacy and data protection to those responsible for overseeing and managing the data protection framework is essential to ensuring that law enforcement authorities using the WAPIS achieve compliance and to reduce risks related to non-compliance. It is important to consider developing compliance, implementation and reporting metrics for the reports for this purpose.

g. Report to external stakeholders such as the data protection authorities, public authorities, other law enforcement authorities and other key stakeholders where necessary. External awareness of the implementation of the data protection framework is key to ensuring openness and transparency. Fostering external awareness among all key stakeholders also builds integrity and provides confidence in the System. Law enforcement authorities using the WAPIS should strive to take a user-centric approach and make transparency a priority by exploring more appropriate ways of fulfilling their obligations. The use of plain language is encouraged. External awareness may be achieved by means of:
   i. Transparency reports generated by the law enforcement authority;
   ii. Filing of data protection compliance audit reports with the data protection authority (where they exist);
   iii. Publication of data protection audit reports;
   iv. Third party verification or accountability audits; and
   v. Creation and updating of a data protection notice.

h. Conduct a risk assessment across all units or departments that access the WAPIS. The data protection risk assessment should be a prerequisite for further development of a general data protection policy. The DPO or relevant officer in the law enforcement authority should create and oversee unit or departmental data protection self-assessments covering reviews, improvements, communications and training for the WAPIS. The risk assessment process will enable the DPO to identify and prioritize data protection gaps within the law enforcement authority and manage policy implementation for risk mitigation in the WAPIS. Where necessary, the law enforcement authorities may consider consulting a competent third party to assist them.

i. Require all WAPIS staff to acknowledge and agree to adhere to the WAPIS data protection framework. This is necessary to ensure that employees or staff understand the purpose of data protection with regard to the implementation and operation of WAPIS. It is important to hold individual employees or staff accountable for their actions with respect to handling personal data. Each employee must therefore be made to acknowledge and agree to adhere to the data protection framework. This can take the form of a separate document (paper or electronic) or be part of an existing document such as the conditions of service, code of conduct, employee handbook or individual copies of the data protection policy.

DATA PROTECTION REGIME AND GOVERNANCE

1. Minimize the risks associated with unauthorized or unlawful processing in the system

2. Define and specify the roles and responsibility of each user of the System

3. Raise awareness and involve high-level administrators in the management of the data protection framework for the WAPIS.

4. Promote an open communication channel between all WAPIS users

5. Prepare reports on data protection issues arising from the functioning of the System

6. Conduct a data protection risk assessment across all units or departments that access the WAPIS

7. **Ensure each WAPIS user signs a data protection undertaking.**

PERSONAL DATA COLLECTION AND SHARING

4.1 COLLECTION OF PERSONAL DATA

1. Prior to collecting personal data, law enforcement authorities should ensure that there is a legal basis for collecting it.
2. The collection of personal data in the System should be limited to what is strictly necessary and proportionate to the law enforcement purposes for which the data are being collected.

CASE STUDY

ON THE NECESSITY OF PERSONAL DATA PROCESSING

Uzun v. Germany, ECHR judgment 2 September 2010, application no. 35629/05

The applicant, suspected of involvement in a bomb attack by a left-wing extremist movement, complained that the surveillance via GPS tracking and the use of the data obtained thereby in the criminal proceedings against him had violated his rights and protections under Article 8 of the ECHR (right to respect for private life).

While the Court recognized that GPS surveillance is, by its very nature, more susceptible to interfere with a person's right to respect for private life (Article 8), such interference is acceptable when such measures are "necessary in a democratic society." The GPS monitoring was not requested or granted at the outset, but was granted after several months of visual surveillance and other less intrusive measures. Additionally, the GPS surveillance only affected him when he was in the vehicle, and thus he could not be said to have been subjected to total and comprehensive surveillance. Finally, because the surveillance was carried out against the background of a serious public threat (attempted bomb attacks against politicians and civil servants), the surveillance was "necessary" within the meaning of Article 8.

3. Where personal data are collected, a clear link between the person whose personal data are processed and the purpose of the processing should be established.

CHAPTER IV

ON THE LINK BETWEEN PERSONAL DATA AND A PERSON

Mustafa Sezgin Tanrikulu v. Turkey, ECHR judgment 18 July 2017, application no. 27473/06

Following a bomb attack that killed a police superintendent, the National Intelligence Agency of Turkey ("MIT") obtained a court order to intercept all domestic and international telephone calls and communications provided between 8 April and 30 May 2005 by Turk Telekom, private mobile network operators and Internet service providers and to obtain information contained in SMS, MMS, GPRS and fax communications, as well as caller IDs, IP address and all other communication-related information.

The ECHR held this order – which authorized the interception of the communications of everyone in the Republic of Turkey – to be unlawful on the basis that, inter alia, it was not limited to people suspected of the relevant criminal offences as required by the applicable law.

4. Law enforcement authorities should make a clear distinction between the various categories of individuals whose data is processed, such as suspects, persons of interest to an investigation, persons convicted of a criminal offence, victims, witnesses, contacts of any of the aforementioned persons, etc.
5. Law enforcement authorities should ensure that data collected are accurate, not misleading, up-to-date, adequate, relevant and not disproportionate to the purposes for which they are being processed.

COLLECTION OF PERSONAL DATA

1. First of all, ensure that there is a legal basis for the collection of personal data

2. Respect the principle of proportionality in the collection of personal data

3. Ensure that data collected are accurate, not misleading, up-to-date, adequate, relevant and not disproportionate to the purposes for which they are being processed

4.2 SHARING OR TRANSMISSION OF DATA TO OTHER PUBLIC BODIES

1. Law enforcement authorities may share or transmit personal data to other public bodies, that are not law enforcement authorities, if:
   a. Such sharing or transmission is provided for by law; and
   b. The data are required by the recipient to enable them to fulfil their lawful task (for example in their investigations or other legal duties in accordance with national law) or to prevent serious and imminent risk to other persons, public order or to public security.
2. On determining whether to share or transmit data to other public bodies, law enforcement authorities should consider the adverse effects that such sharing or transmission may have on an individual.
3. Law enforcement authorities should inform the receiving public body of their obligation to use the shared or transmitted data solely for the purposes for which the data were shared or transmitted.
4. Law enforcement authorities should ensure that the public bodies have taken the necessary steps to comply with the applicable data protection framework.

SHARING/TRANSMISSION OF DATA

1. Before sharing/transmitting personal data to other bodies, ensure that such sharing/transmission is provided for by law

2. Before sharing or transmitting data to other bodies, consider the adverse effects that such sharing or transmission may have on an individual

3. Inform the receiving public body of their obligation to use the shared or transmitted data solely for the purposes for which the data were shared or transmitted.

4.3 SHARING OR TRANSMISSION OF DATA TO PRIVATE BODIES OR THE PUBLIC

1. Law enforcement authorities may, in accordance with the applicable law in each country, share or transmit personal data to private bodies in one or more of the following instances:
   a. In furtherance of law enforcement purposes;
   b. To prevent serious and imminent risk to public order or public security;
   c. In the interests of the data subject; and
   d. For humanitarian reasons.
2. In determining whether to share or transmit personal data to other private bodies, law enforcement authorities should consider the adverse effects that such sharing or transmission may have on an individual.
3. When personal data is shared or transmitted to a private body, the law enforcement authority should ensure that the private body provides a written undertaking that it shall comply with the applicable data protection principles.
4. When sharing or transmitting personal data to the public in relation with an investigation, special consideration should be given to the necessity and public interest of sharing or transmitting information in this way. Appropriate safeguards should be put in place to ensure the respect of the rights of the individuals involved in the case.
5. Sharing or transmission of data to the public should be for the purpose of:
   a. Alerting the public;
   b. Requesting help from the public; or
   c. For any other law enforcement purpose as defined in point 2.2 above.
6. Where a law enforcement authority has received personal data from another law enforcement authority, it should obtain their formal consent prior to sharing or transmitting that personal data to a private body or to the public.

7. The sharing or transmitting law enforcement authority must make appropriate arrangements to ensure the shared or transmitted personal data is subject to an equivalent or a higher level of protection.

BEST PRACTICE

SHARING OR TRANSMISSION OF DATA TO PRIVATE BODIES OR THE PUBLIC

1. Comply with the terms of applicable legal texts before sharing or transmitting personal data to private bodies

2. Consider the adverse effects that sharing or transmitting personal data may have on victims or witnesses before sharing or transmitting the data

3. Inform victims and witnesses before sharing or transmitting their personal data to the public

4. Respect the rights of individuals when sharing or transmitting their personal data to the public

5. Obtain the formal consent of the law enforcement authority prior to sharing or transmitting personal data to a private body or to the public

6. Ensure that a sufficient level of protection will be given to personal data before sharing or transmitting that data to private bodies or to the public

7. Ensure private bodies sign a written undertaking to respect principles applicable to personal data protection.

ON TRANSMISSION OF PERSONAL DATA TO MEMBERS OF THE PUBLIC

West Midlands Police, ICO Undertaking, Ref. ENF0674010

A Criminal Behaviour Order (CBO) for damaging property and threatening violence was imposed on two individuals. It prohibited them from entering certain premises and associating with one another in certain areas. The West Midlands Police (Data Controller) decided to publicise the terms of this order in a leaflet distributed to roughly 30 homes which included personal data of the victims and witnesses of the crimes without their permission. The Information Commissioner (Data Protection Authority) required the data controller to ensure that:

- Risk assessments were carried out in relation to victims and witnesses of offences during the publication of CBOs;
- Victims and witnesses are informed before publication of materials;
- The creation and distribution procedure is documented;
- Mandatory data protection training is given to all new and existing staff members who process personal data;
- Refresher data protection training is provided for all staff members who process personal data;
- Systems are introduced to monitor the uptake of data protection training; and
- Implementation takes place within three months.

4.4 SHARING OR TRANSMISSION OF DATA INTERNATIONALLY

1. As a general rule, law enforcement agencies sharing or transmitting data internationally should consider whether the receiving authority is performing a function conferred upon it by law for law enforcement purposes, and whether the sharing of data is necessary for it to perform its law enforcement duties. International transfer of personal data should be limited to law enforcement authorities.
2. When sharing or transmitting personal data to a law enforcement authority in a third country or to a regional or international organization, the sharing or transmitting authority should ensure that the country and/or law enforcement authority provides an adequate level of protection regarding the security of information, privacy, freedoms and the fundamental rights of individuals in relation to the processing of such data.
3. The sharing or transmitting law enforcement authority must take reasonable measures to ensure an equivalent or higher level of protection for the shared or transmitted data.

BEST PRACTICE

SHARING OR TRANSMISSION OF DATA INTERNATIONALLY

8. Comply with the terms of legal texts before sharing or transmitting personal data internationally

9. Ensure that the country and/or law enforcement authority provides an adequate level of protection when processing the data