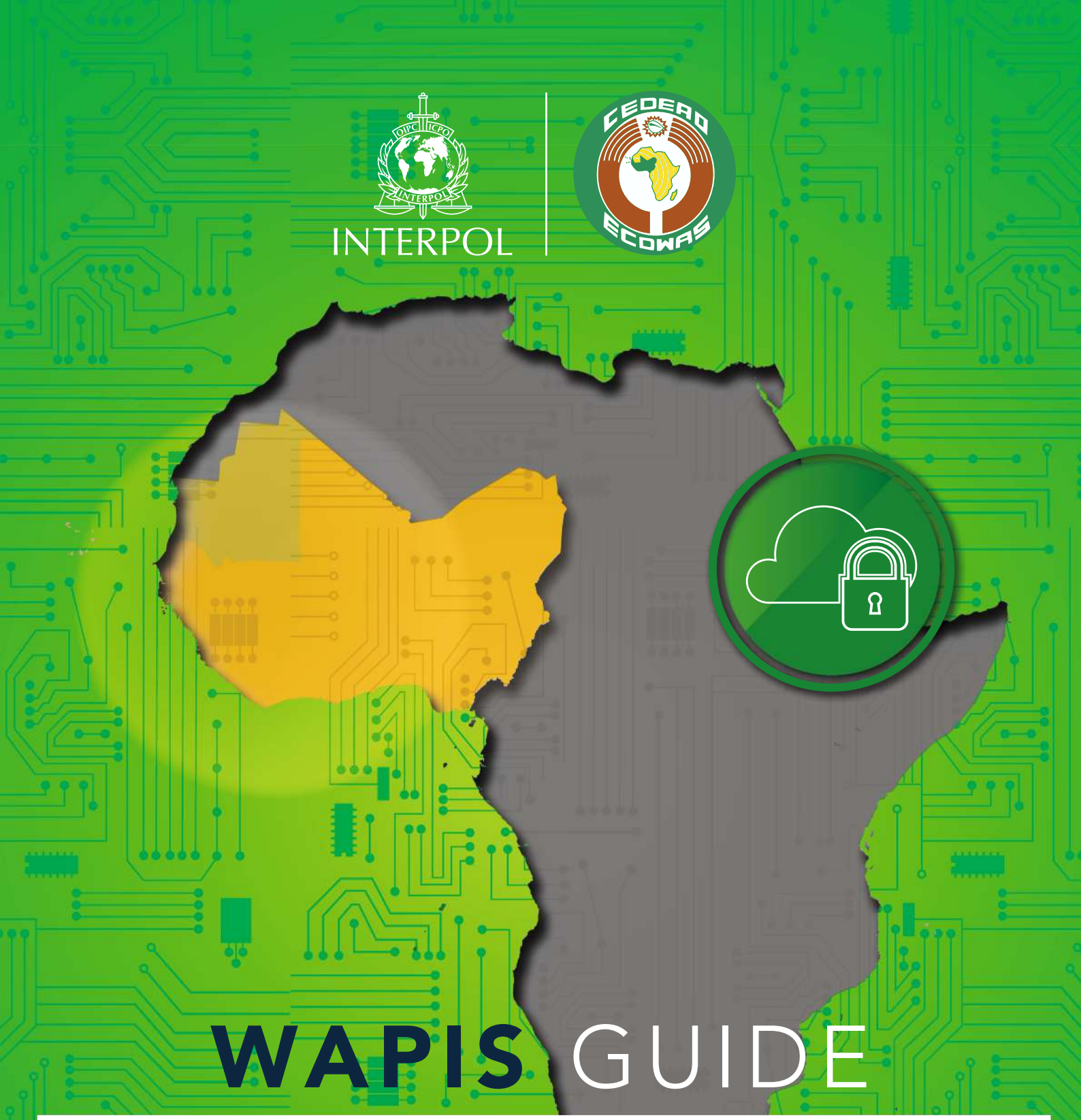
INTERPOL



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

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

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

BEST PRACTICE

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.

BEST PRACTICE

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.**

CHAPTER IV

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.

CASE STUDY

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.

BEST PRACTICE

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.

BEST PRACTICE

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.

CASE STUDY

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

CHAPTER V

DATA QUALITY, CONFIDENTIALITY AND SECURITY

5.1 DATA QUALITY

1. Law enforcement authorities should take all reasonable steps to ensure that personal data that are inaccurate, incomplete or no longer up-to-date are not transmitted, shared or made available. To this end, law enforcement authorities should verify the quality of personal data before they are transmitted, shared or made available.
2. Insofar as possible, in all transmissions or sharing of personal data, information enabling the recipient to assess the degree of accuracy, completeness and reliability of the personal data and the extent to which such data is up-to-date should be provided.
3. In the event of inaccurate or incorrect personal data being shared or transmitted or unlawful sharing or transmission of personal data, the recipient should be notified without delay. In such a case, the personal data should be rectified, erased or processed in a restricted manner as appropriate.
4. Data collected should be distinguished according to the degree of accuracy or reliability and, in particular, data based on facts should be distinguished from data based on opinions or personal assessments.

CASE STUDY

ON THE PROCESSING OF INCORRECT PERSONAL DATA

Cemalettin Canli v. Turkey, ECHR judgment 18 November 2008, application no. 22427/04

In 2003, while criminal proceedings were pending against Cemalettin Canli, police authorities submitted a police report mentioning two previous sets of criminal proceedings from 1990 referring to his membership of an illegal organization. Canli had been acquitted on one charge and the criminal proceedings for the other charge had been discontinued.

The court found that the police report did not abide by the law due to its failure to mention Mr. Canli's acquittal and discontinuation of criminal proceedings.

Mikolajova v. Slovokia, ECHR judgment 18 January 2011, application no. 4479/03

In 2000, a criminal complaint was brought against the applicant by her husband who claimed he had been abused by her. The charges were dropped several days later and the complaint never reached court. However, the police recorded that the applicant had committed a criminal offence by inflicting bodily harm and disclosed this information to a third party, which used this information to the applicant's detriment. The court found that the police decision violated the applicant's rights because it was framed in a way that indicated the applicant to be guilty, despite the fact that she had never been charged or proven to be guilty of the offence.

BEST PRACTICE

DATA QUALITY

1. Verify the quality of personal data before they are transmitted, shared or made available

2. Notify recipients in the event of inaccurate or incorrect data being shared, transmitted or made available

3. **Distinguish data according to the degree of accuracy or reliability.**

5.2 CONFIDENTIALITY AND SECURITY

1. Law enforcement authorities should take appropriate, reasonable, technical and organisational measures to secure the System against risks such as accidental or unauthorized access to, destruction, loss, use, alteration or disclosure of personal data.
2. Law enforcement authorities should implement measures designed to:
   - **a.** Deny unauthorized persons access to the System's equipment used for processing data;
   - **b.** Prevent the unauthorized reading, copying, alteration or removal of data from the System;
   - **c.** Prevent unauthorized input of personal data and the unauthorized consultation, alteration or erasure of stored personal data;
   - **d.** Prevent the use of automated processing systems by unauthorized persons using data communication equipment;
   - **e.** Ensure that persons authorized to use the System only have access to the personal data covered by their access authorization;
   - **f.** Ensure that it is possible to verify and establish to which bodies personal data in the System have been or may be transmitted or made available;
   - **g.** Ensure that it is subsequently possible to verify and establish which personal data have been input into the System, when and by whom;
   - **h.** Prevent the unauthorized reading, copying, alteration or erasure of personal data during transfers of personal data or during transportation of data media;
   - **i.** Ensure that in the event of interruption it is possible to quickly restore the System; and
   - **j.** Ensure that the System operates smoothly, that any malfunctions are reported and that stored personal data cannot be corrupted due to a system malfunction.
3. Personal data sent or managed by subcontractors should be subject to sufficient confidentiality guarantees.

CASE STUDY

ON ACCIDENTAL DISCLOSURE OF PERSONAL DATA

Gloucestershire Police, ICO Monetary Penalty, 11 June 2018

On 19 December 2016, an officer investigating non-recent child abuse cases sent an email to 56 recipients without using the BCC feature, allowing all (at least 52) of the recipients to see email addresses associated with victims, journalists and lawyers. The email was recalled on 21 December 2016, and the matter was reported to the data protection authority. The data protection authority found the following:

- Police failed to send separate emails to each participant and instead utilized the bulk email facility;
- Police failed to use the Microsoft Outlook BCC function;
- Police failed to provide staff with any (or any adequate) policies, guidance or training on bulk email communication and the use of the BCC functionality in Outlook, particularly in cases where emails were being sent to multiple victims of sensitive or live cases; and
- Police communicated with data subjects and the data protection authority immediately as required.

The data protection authority imposed a monetary penalty of GBP 80,000 after taking into account certain mitigating factors, including the fact that the police notified data subjects immediately, several of the recipients were already acquainted, the data protection authority was notified immediately, and the department was in the process of improving its technical and organizational measures to prevent similar occurrences in the future.

CASE STUDY

CASE STUDY ON MALICIOUS INPUT OF PERSONAL DATA

CNBC, 'Immigration Officer Fired After Putting Wife on List of Terrorists to Stop Her Flying Home', 1 February 2011

A British immigration officer tried to rid himself of his wife by adding her name to a list of terrorist suspects. He used his access to security databases to include his wife on a watch list of people banned from boarding flights into Britain because their presence in the country is 'not conducive to the public good'. As a result, the woman was unable to return from Pakistan for three years after travelling to the county to visit family. The tampering went undetected until the immigration officer was selected for promotion and his wife's name was found on the suspects' list during a vetting inquiry. The Home Office confirmed that the officer had been sacked for gross misconduct.

BEST PRACTICE

CONFIDENTIALITY AND SECURITY

1. Ensure the integrity of the System
2. Put in place a security policy
3. Ensure the confidentiality of the data in the System
4. Report faults in the System
5. Take emergency technical and organizational measures in case of system failure

CHAPTER VI

CASE STUDY

BEST PRACTICE

DATA BREACHES

6.1 DATA BREACH NOTIFICATION

1. Law enforcement authorities should document all personal data breaches liable to pose a risk to the rights and freedoms of natural persons.
2. In the event of a personal data breach liable to pose a risk to the rights and freedoms of natural persons, the law enforcement authority – through its designated Data Protection Officer – should notify the data protection authority of the breach, without undue delay and, where feasible, no later than 72 hours after having become aware of it. The data breach notification to the data protection authority should:
   a. Describe the nature of the personal data breach including, where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;
   b. Communicate the name and contact details of the data protection officer or other contact point where more information can be obtained;
   c. Describe the likely consequences of the personal data breach; and
   d. Describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.
3. Where a law enforcement authority has shared or transmitted data to a recipient in another country, the information in point 2 above should be communicated to the recipient.

6.2 DATA BREACH NOTIFICATION TO DATA SUBJECT

1. In the event of a personal data breach liable to pose a risk to the rights and freedoms of natural persons, the law enforcement authorities should communicate the personal data breach to the data subject without undue delay. The law enforcement authority should:
   a. Communicate the name and contact details of the data protection officer or other contact point where more information can be obtained to the data subject;
   b. Describe the likely consequences of the personal data breach;
   c. Describe the actual or proposed measures to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.
2. The communication to the data subject described above is not required if:
   a. The law enforcement authority has implemented appropriate technological and organisational protection measures which were applied to the personal data affected by the personal data breach, in particular those that render the

personal data unintelligible to any person who is not authorized to access it, such as encryption;

b. The law enforcement authority has taken subsequent measures to mitigate the potential risk to the rights and freedoms of data subjects; and

c. It would involve a disproportionate effort. In such a case, the law enforcement authority should instead issue a public communication or take an equally effective measure to notify the subject.

3. Communication to the data subject may be delayed, restricted or withheld if it is a necessary and proportionate measure with due regard to the fundamental rights and the legitimate interests of the natural person concerned in order to:

a. avoid obstructing official or legal inquiries, investigations or procedures;

b. avoid prejudicing the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties;

c. protect public security;

d. protect national security;

e. protect the rights and freedoms of others.

CASE STUDY

ON DATA BREACH NOTIFICATION TO A DATA SUBJECT AND DATA PROTECTION AUTHORITY

Crown Prosecution Service, ICO Monetary Penalty, 14 May 2018

The police sent the Crown Prosecution Service (CPS) DVDs containing interviews with victims of child sexual abuse which went missing following delivery. Both the data subjects and Data Protection Authority were informed. The DVDs were not encrypted, though the CPS had the possibility to do so, nor were the DVDs shipped in tamper-proof packaging. The Data Protection Authority found the following:

- The CPS did not intentionally occasion the loss but should have been aware of the risk of loss;
- The CPS had dealt with these kinds of interviews before, and was guilty of a similar breach in relation to failing to properly secure recordings of victims and witnesses in sexual abuse cases;
- The CPS failed to take reasonable steps to prevent the loss, such as transporting encrypted DVDs in sealed, tamper-proof packaging, using a secure courier service with signature upon delivery, and ensuring deliveries to a secure location;
- The CPS failed to notify the data subjects of the breach immediately;
- The CPS failed to notify the data protection authority of the breach immediately as required;
- The CPS was slow to escalate the issue to appropriate management levels; and
- The DVDs had still not been recovered.

The data protection authority imposed a monetary penalty of GBP 200,000.

BEST PRACTICE

DATA BREACH NOTIFICATION

1. Notify the Data Protection Authority and the data subjects in the event of a data breach

2. Inform the Data Protection Authority and data subjects of the measures taken or proposed measures to address the personal data breach

3. Promptly notify the Data Protection Authority and data subject.

CHAPTER VII

PROCESSING RECORDS AND DATA RETENTION

7.1 RECORDS OF PROCESSING ACTIVITIES

1. Law enforcement authorities should maintain records of all categories of processing activities under their responsibility containing:
   - **a.** Names and contact details of the person(s) in charge of the System in the country and the data protection officer;
   - **b.** The purpose of processing;
   - **c.** Categories of recipients to whom personal data have been or will be disclosed including recipients in third countries or international organisations;
   - **d.** A description of the categories of data subjects and of the categories of personal data;
   - **e.** Where applicable, the use of profiling;
   - **f.** Where applicable, the categories of transfers of personal data to a third country or an international organisation;
   - **g.** An indication of the legal basis for the processing operation, including transfers, for which the personal data are intended;
   - **h.** Where possible, the envisaged time limits for erasure of the different categories of personal data; and
   - **i.** Where possible, a general description of the technical and organisational security measures applicable to the System.

7.2 LOGS

1. Law enforcement authorities should keep logs of the following processing operations:
   - **a.** Collection;
   - **b.** Alteration;
   - **c.** Access/Consultation;
   - **d.** Disclosure including transfers;
   - **e.** Combination; and
   - **f.** Erasure.
2. The logs of consultation and disclosure should make it possible to establish, in case of consultation or disclosure, the justification, date and time of such operations and the identification of the person who consulted or disclosed personal data, and the identity of the recipients of such personal data.
3. The logs should be used solely for the verification of the lawfulness of processing, self-monitoring and ensuring the integrity and security of the personal data and for criminal proceedings. Law enforcement authorities should make the logs available to the data protection authority on request.

4. The logs should only be assessed by a person with the accredited role of "auditor" in the System and only through the System.
5. The logs may be modified or erased in accordance with policies and or acceptable best practice.

7.3 DATA RETENTION

1. Law enforcement authorities should develop internal rules and/or recommendations setting the data retention period for personal data or for a periodic review of the need for the storage of personal data.
2. Law enforcement authorities should periodically review the grounds for retention and processing of personal data.
3. In order to determine the appropriate period for retention of the personal data in the System, the law enforcement authorities should:
   a. Review the length of time personal data is kept on the basis of the applicable national legislation, nature of the data, its policies and best practice;
   b. Consider the specified purpose for the information before deciding whether (and for how long) to retain personal data;
   c. Securely delete information that is no longer needed for specified purposes; and
   d. Update, archive or securely delete information if it becomes out-of-date.
4. The data processed in the System should only be stored for as long as necessary for the law enforcement authorities concerned to fulfil their purpose.

CASE STUDY

ON DATA RETENTION

Brunet v. France, ECHR judgment 18 August 2014, application no. 21010/10

Brunet and his partner were engaged in a violent altercation and Brunet was taken into custody. Brunet and his partner wrote to the prosecutor expressing disagreement with the charges and the criminal proceedings were discontinued. However, Brunet's personal data was retained in the database in connection with the altercation, and was to be maintained there for 20 years. After several unsuccessful attempts to erase his information from the database, the prosecutor informed Brunet that he was unable to ascertain whether Brunet's information could be erased from the list.

The Court held that, because the database contained identity and personality traits for the purposes of researching crime, maintaining Brunet's information in such a database for 20 years was excessive, especially in light of the fact that the charges had been dropped and there had been no criminal proceedings. Additionally, because the prosecutor was unable to ascertain the appropriateness of retaining such data, Brunet had no real opportunity to request the erasure of his data.

BEST PRACTICE

DATA RETENTION

1. Develop internal rules and/or recommendations setting the data retention period for personal data or for a periodic review of the need for the storage of personal data

2. Law enforcement authorities should periodically review the grounds for retention and processing of personal data

3. Ensure that data is stored only for as long as necessary for the law enforcement authorities concerned to fulfil their purpose.

CHAPTER VIII

SENSITIVE DATA PROCESSING

8.1 SENSITIVE DATA PROCESSING

1. 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 ('sensitive data') should not be processed in the System except where strictly necessary, subject to appropriate safeguards for the rights and freedoms of the data subject, and only:
   a. Where authorized by ECOWAS regulations or those of the WAPIS participating country;
   b. To protect the vital interests of the data subject or of another natural person; or
   c. Where such processing relates to data which are made public by the data subject.

CASE STUDY

ON SENSITIVE PERSONAL DATA PROCESSING

Humberside Police, ICO Monetary Penalty, 28 March 2018

The police misplaced three disks containing an interview with an alleged rape victim. The disks were the only copies and contained sensitive and personal data of the alleged victim and alleged perpetrator including full names, birth dates, and the mental health and treatment of the alleged victim. The only written notes detailing the interview were included with the disks. The disks were discovered missing 14 months after the interview. The victim was notified and was unwilling to participate in any further interviews with police. The disks were not recovered. The data protection authority found:

- The police failed to ensure the disks were encrypted for transferring outside the police force area;
- The police failed to make working copies of the disks when transferring outside the police force;
- The police failed to adhere to existing policies regarding information security;
- The police failed to maintain an audit trail of the disks' whereabouts;

- The police failed to provide an adequate data protection training and monitoring programme to officers; and
- The police failed to make existing policies and procedures regarding storage and transfer of data more robust.

The data protection authority issued a monetary penalty of GBP 130,000.

BEST PRACTICE

SENSITIVE DATA PROCESSING

1. Respect the rights and freedoms of data subjects before collecting sensitive data
2. Make existing policies regarding the security of sensitive information more robust.

CHAPTER IX

DATA SUBJECT RIGHTS

9.1 RIGHT TO ACCESS

1. Where a data subject has had their data processed in the System for law enforcement purposes, as soon as circumstances safely permit, the law enforcement authority should permit the data subject to either directly or indirectly access the data at their request subject to the applicable legal framework.
2. In respect of direct access, the data subject can directly request access from the law enforcement authority responsible for the data. The law enforcement authority should assess the request and any possible restriction or derogation which can only be applied if necessary for a law enforcement purpose or for the protection of the data subject or the rights and freedoms of others, and reply directly to the data subject.
3. In respect of indirect access, the data subject should make his/her request to the data protection authority, which may carry out the request on their behalf and conduct checks regarding the lawfulness of the processing of the data subject's personal data, and the availability of the same. The data protection authority may then respond to the data subject as appropriate.
4. If a WAPIS participating country does not have a functioning data protection authority or oversight body, and until such a body is established, the right of access should be direct, subject to the applicable legal framework.
5. Where a WAPIS participating country has a functioning data protection authority whose legal framework allows a data subject to exercise the right to indirect access to their personal data through it, the right to direct access may be restricted.
6. Where necessary and proportionate, the right to access may be exceptionally limited or excluded, wholly or partly, in accordance with the applicable legal framework, in order to:
   a. Avoid obstructing official or legal inquiries, investigations or procedures;
   b. Avoid prejudicing the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties;
   c. Protect the rights and freedoms of others;
   d. Safeguard an ongoing investigation, prosecution or another important law enforcement task;
   e. Protect State interests (such as public security and national security).
7. Where the right to access is limited or excluded, the law enforcement authority or data protection authority should inform the data subject, without undue delay, in writing about the reasons for refusal or restriction of access. Such reasons may be omitted where their provision would undermine a purpose

under paragraph 6 above. The law enforcement authority should inform the data subject of their entitlement to lodge a complaint with the data protection authority or seek a judicial remedy, as appropriate.

8. The right of access should, in principle, be free of charge. A reasonable administrative fee for the request may be charged if national law permits.
9. The law enforcement authority should stipulate in a policy or notice a reasonable timeframe within which it will address access requests.

CASE STUDY

ON RIGHT TO ACCESS

Segerstedt-Wiberg and others v. Sweden, ECHR judgment 6 June 2006, application no. 62332/00

The applicants in this case attempted to gain access to their personal data contained in Swedish Security Police files. The case concerns five individuals: Segerstedt-Wiberg, Nygren, Ehnebom, Frejd, and Schmid. The state relied on the 1980 Secrecy Act to withhold information stating it was "not clear that the information may be imparted without jeopardising the purpose of the decision or measures planned or without harm to future activities."

Segerstedt-Wiberg was a prominent Liberal Member of Parliament and requested access to the police records after damaging information was circulated about her, including rumours that she was "unreliable" in respect of the Soviet Union. The police released all information about Segerstedt-Wiberg up until 1976, but maintained restrictions on the rest of the file due to continued threats against her. The Court accepted that the storage of the information was for a legitimate purpose (the prevention of disorder or crime) and found no reason to doubt the state's decision to withhold information from her in light of security threats against her (e.g. a bomb threat from 1990).

Nygren was a journalist who had written a number of articles about Nazism and the Security Police. He was given access to two pages of his file, but the rest of his request for access to his file was denied. The Court held that the nature and age of the information did not justify the continued storage as regards the protection of national security.

Ehnebom was a member of a communist party. He was granted access to 30 pages of his file and claimed that the information contained therein was responsible for the call for his removal from his post. Frejd was also a member of a communist party and was well known in sports circles throughout Sweden. He was granted permission to see parts of his file regarding his participation in the organization, including a bid for election as a party member.

However, he was denied access to the entirety of his file. In both of these cases, the Court acknowledged that the two men were members of an organization advocating armed opposition and the establishment of one group over another, however this was the only evidence used by the government for retaining the personal data.

Schmid was a member of the European Parliament and belonged to the Swedish Left Party. He was given access to selected files concerning political movements regarding nuclear disarmament and membership of Social Democrat groups. The Court found no reason to justify the retention nor the restriction of the record in the interest of Swedish national security, thus concluding that the continued storage of the information was disproportionate to the legitimate aims of the law.

9.2 RIGHT TO RECTIFICATION OR ERASURE

1. Data subjects may directly or indirectly request law enforcement authorities to rectify or erase inaccurate personal data relating to them that is contained in the System, in accordance with the applicable legal framework of the WAPIS participating country. The data subjects may also request to have incomplete personal data completed.
2. In respect of the direct exercise of this right, the data subject can request rectification or erasure directly from the law enforcement authority responsible for the data. The law enforcement authority should assess the request and any possible restriction or derogation which can only be applied if necessary for a law enforcement purpose, or is necessary for the protection of the data subject or the rights and freedoms of others, and reply directly to the data subject.
3. In respect of the indirect exercise of this right, the data subjects should make their request for rectification or erasure to the data protection authority, which may carry out the request on their behalf and conduct checks regarding the availability and lawfulness of the processing of the data subject's personal data. The data protection authority may then respond to the data subject as appropriate.
4. If a WAPIS participating country does not have a functioning data protection authority, the right to rectification or erasure should be exercised directly with the law enforcement authority, subject to the applicable legal framework.

5. Where a WAPIS participating country has a functioning data protection authority or oversight body whose legal framework allows a data subject to exercise the right to rectification or erasure indirectly through it, the right to directly request rectification or erasure may be restricted.
6. Instead of erasure, law enforcement authorities should restrict processing where:
   a. The accuracy of the personal data is contested by the data subject and their accuracy or inaccuracy cannot be ascertained; or
   b. The personal data must be maintained for evidentiary purposes.
7. The law enforcement authority or the data protection authority, as the case may be, should inform the data subject in writing of any refusal of rectification or erasure of personal data or restriction of processing and of the reasons for refusal.
8. In accordance with the applicable, laws, the law enforcement authority may restrict, wholly or partly, its obligation to provide such information to the extent that such a restriction is necessary and proportionate with due regard for the fundamental rights and legitimate interests of the data subject and applicable laws, in order to:
   a. Avoid obstructing official or legal inquiries, investigations or procedures;
   b. Avoid prejudicing the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties;
   c. Protect the rights and freedoms of others;
   d. Safeguard an ongoing investigation, prosecution or another important law enforcement task;
   e. Protect State interests (such as public security and national security).
9. Where a law enforcement authority has rectified, erased or restricted the processing of personal data, the law enforcement authority should notify all recipients to whom it has transferred such data of this fact and ask the recipients to do likewise.

CASE STUDY

ON THE RIGHT TO RECTIFICATION OF PERSONAL DATA

Khelili v. Switzerland, ECHR 18 October 2011, application no. 16188/07

In 1993, the Geneva police entered information regarding Ms. Khelili in the police database containing the word "prostitute." The law allowed the police to manage records as long as the data was necessary to enable them to carry out their duties (i.e. punish offences and prevent crime). In 2001, 2002, and 2003, unrelated criminal complaints were lodged against Ms. Khelili for insulting and threatening behaviour. During this time, Ms. Khelili discovered the police maintained the word "prostitute" in her file. In 2006, she requested the word be removed from her record and was informed by the police chief that it had been. However, while the 1993 record had been expunged, the word "prostitute" remained in connection with the 2001, 2002, and 2003 complaints.

The court agreed that the recording of the word "prostitute" in Ms. Khelili's police file was an interference in accordance with the law for the purpose of preventing disorder and crime and for the protection of the rights of others. While the word "prostitute" as a profession had been deleted from the police database, it had not been corrected in connection with criminal proceedings relating to the other complaints against Ms. Khelili and could damage her reputation both in private and public. The Court considered first the fact that the allegations of prostitution were vague and general, and the connection between the 1993 record and the charges from 2001, 2002 and 2003 were not sufficiently close. Next it noted the police had erased "prostitute" from part but not all of her record, while informing Ms. Khelili that they had expunged the word "prostitute" from her record. Thus the police were storing false data concerning Ms. Khelili and the retention of the word "prostitute" in her file was neither justified nor necessary in a democratic society.

BEST PRACTICE

DATA SUBJECT RIGHTS

1. Respect the exercise of the right to access of data subjects

2. Respect the exercise of the right to rectification and erasure of inaccurate personal data recorded in the System

CHAPTER X

DATA PROTECTION IMPACT ASSESSMENT

10.1 DATA PROTECTION IMPACT ASSESSMENT

1. Law enforcement authorities should complete and document a data protection impact assessment to record the risks identified and the measures that have been implemented to manage these risks.
2. Where necessary a data protection impact assessment should be conducted prior to implementing the System and at regular intervals.
3. The impact assessment should identify and take into consideration:
   a. Information on what data will be, or is being, processed;
   b. Persons or category of persons whose data will be, or is being, processed;
   c. The type of processing, including a timeline of the data from collection to deletion;
   d. The risks associated with the processing;
   e. The measures taken to manage the identified risks;
   f. The legal regimes/obligations which apply, if any;
   g. The direction provided by data protection authorities;
   h. Any residual risks, or measures that cannot be managed or implemented and the justification and acceptance of such risks.
4. For the purposes of data protection impact assessment, law enforcement authorities should develop a risk-based approach to the WAPIS data protection programme based on best practices as well as legal and regulatory compliance risks. To this end, law enforcement authorities should:
   a. Understand data protection risks in the WAPIS, its overall organisational goals, culture, language and operations;
   b. Identify areas where personal data are likely to be collected, processed or used within the WAPIS;
   c. Based on identified data protection risks, determine data protection priorities to align with its overall goals.

BEST PRACTICE

IMPACT ASSESSMENT

Conduct a data protection impact assessment before implementing the System and thereafter at regular intervals

Verify whether the processing of data is likely to pose a heightened risk for the rights and freedoms of data subjects.

CHAPTER XI

EXCEPTIONS

11.1 EXCEPTIONS FROM THE PROCESSING OF DATA IN ACCORDANCE WITH THIS GUIDE

1. Exceptions to the processing of data in accordance with this guide should only be invoked if:
   a. They are provided for expressly by law; and
   b. Constitute a necessary and proportionate measure for the purpose of the protection of national security, defence, public safety, important economic and financial interests, impartiality and independence of the judiciary, the prevention, investigation and prosecution of criminal offences, the execution of criminal penalties, protection of essential objectives in the public interest, or protection of the rights and fundamental freedoms of others.
2. If an exception defined by national law providing specific safeguards is invoked by law enforcement authorities, it should be used for legitimate aims and only to the extent necessary and proportionate to achieve the aim for which it is being used. It should be limited to cases where not invoking such exceptions would endanger the law enforcement purpose of the processing of data.

CHAPTER XII

CONCLUSION

This document is not intended to be a law or regulation. It is a reference document that will guide law enforcement authorities on the practical application of data protection principles required by law or as a self-regulatory measure under circumstances where no data protection law exists. If it is followed, it will enable WAPIS participating countries to adopt best practices that will facilitate information sharing and maximise the use of the System. It can also widen its data protection implementation scope beyond the System to cover all operations of a law enforcement authority.

KEY TAKEAWAYS

INTRODUCTION

The Heads of State and Government of the Member States of the Economic Community of West African States ("ECOWAS") signed the Supplementary Act A/SA.1/01/10 on Personal Data Protection within ECOWAS ("the Act") on 16 February 2010.

The Act:

- establishes fundamental principles applicable to the processing of personal data in the West African Police Information System ("WAPIS"); and
- directs member states to enact data protection legislation and establish data protection authorities.

CHAPTER I – GENERAL TERMINOLOGY

The first chapter provides an overview of terminology used in the Guide. It identifies:

- Who must comply with the Act? Data Controllers and Data Processors
- Who receives personal data? The Recipients
- Who is the subject of the personal data processing? Data Subjects
- What type of information is regulated under the Act? Personal Data

CHAPTER II – PRINCIPLES AND PURPOSE

The second chapter presents general personal data protection principles and legitimate law enforcement purposes for processing data.

2.1 – Applicable Personal Data Protection Principles.

The protection principles include the principles of:

- **Legitimacy**
- **Legality and Fairness**
- **Purpose, Relevance and Preservation**
- **Accuracy**
- **Transparency**
- **Confidentiality and Security**
- **Choice of the Data processor**

› 2.2 – Purpose of Processing Data in the System.

Law enforcement authorities should be aware of the situations where they can process data in WAPIS. They may do so for the following purposes:

- 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; and
- any duty or responsibility of law enforcement authorities arising from law.

CHAPTER III – DATA PROTECTION REGIME AND GOVERNANCE

The third chapter discusses the data protection authorities, data protection awareness and training, and general compliance.

› 3.1 – Control and Notification

All WAPIS participating countries should establish an independent data protection authority that is responsible for all data processing operations.

› 3.2 – Data Protection Officer ("DPO") and Data Protection Awareness Training

Law enforcement authorities should designate a Data Protection Officer to:

- advise law enforcement authorities of legal obligations;
- monitor compliance;
- provide advice concerning data protection impact assessments;
- liaise with data protection authorities; and
- implement suitable ongoing training to WAPIS users.

› 3.3 – Data Protection Compliance and Governance

Law enforcement authorities should incorporate data protection into their governance structures by engaging all key stakeholders in the WAPIS data protection framework.

CHAPTER IV – PERSONAL DATA COLLECTION AND SHARING

The fourth chapter lays out best practices for the collection and sharing of personal data.

› 4.1 – Collection of Personal Data.

In general, the collection of personal data should be limited to what is necessary and proportionate to the law enforcement purposes for which the data are collected.

4.2 – Sharing or Transmission of Data to other Public Bodies.	Once personal data are collected, law enforcement authorities may share personal data with other public bodies (not including law enforcement authorities) if such sharing is provided for by law and the data are required by the recipient to enable them to perform their lawful duties.
4.3 – Sharing or Transmission of Data to Private Bodies or the Public.	Once personal data are collected, law enforcement authorities may share personal data with private bodies if sharing is, in furtherance of law enforcement purposes, necessary to prevent a serious and imminent risk to public security, in the interests of the data subject, or for humanitarian reasons. Once personal data are collected, law enforcement authorities may share personal data with the public if it is being used for the purpose of alerting the public, requesting help from the public or for any other law enforcement purpose.
4.4 – Sharing or Transmission of Data Internationally.	Once personal data are collected, law enforcement authorities may share personal data with International Law Enforcement Authorities or International Organizations if: (a) the receiving authority is performing a function conferred upon it by law for law enforcement purposes; (b) sharing the data is necessary for it to perform its law enforcement duties; and (c) the sharing authority ensures that the receiving authority applies an adequate level of protection for the security of information in relation to the processing of such data.

CHAPTER V – DATA QUALITY, CONFIDENTIALITY AND SECURITY

The fifth chapter provides an overview of data quality and the measures law enforcement authorities should implement to ensure personal data remains confidential and secure.

› 5.1 – Data Quality

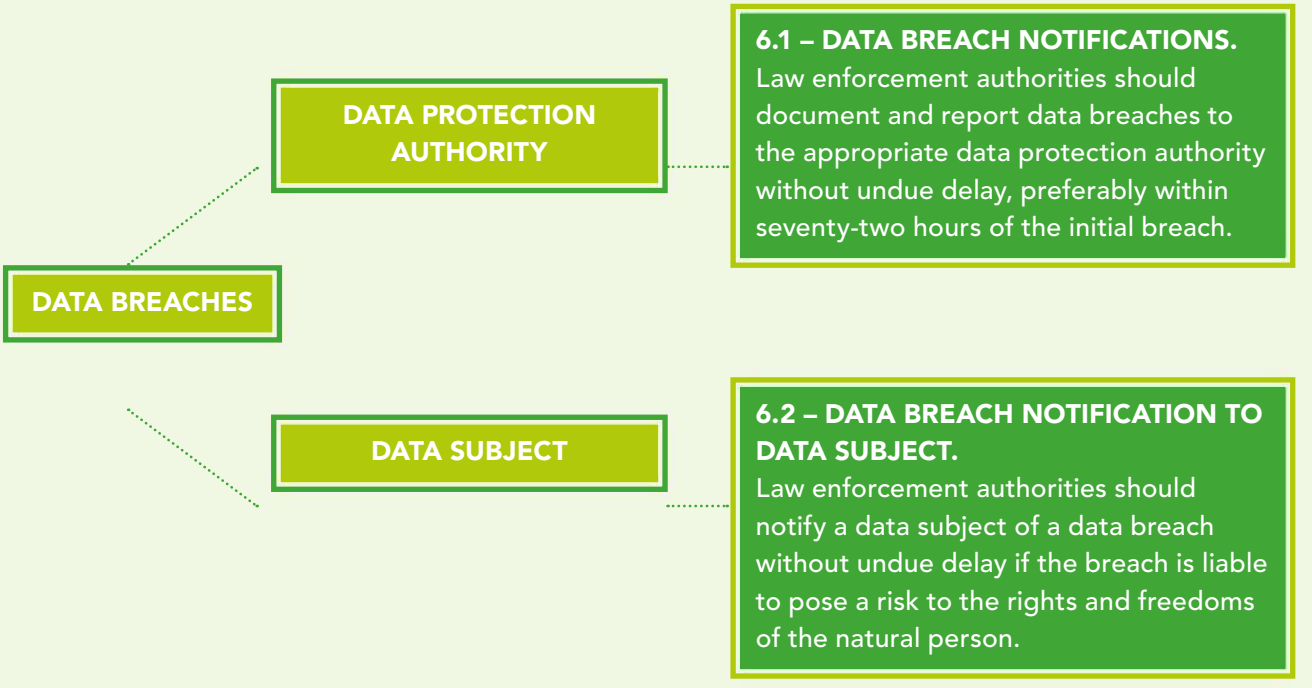
Law enforcement authorities should not share inaccurate, outdated, or incomplete personal data. If inaccurate personal data are shared, law enforcement authorities should notify the recipient without delay and take appropriate steps to rectify, erase or restrict the processing of the data.

› 5.2 – Confidentiality and Security

Law enforcement authorities should take appropriate, reasonable technical measures to secure WAPIS against risks of accidental or unauthorized access to, destruction, loss, use, alteration or disclosure of personal data.

CHAPTER VI – DATA BREACHES

The sixth chapter describes the appropriate steps law enforcement authorities should take in the event of a data breach.



CHAPTER VII – PROCESSING RECORDS AND DATA RETENTION

The seventh chapter outlines best practices for processing records and data retention.

› **7.1 – Records of Processing Activities**

Law enforcement authorities should maintain records of all data processing activities.

› **7.2 – Logs**

Law enforcement authorities should keep logs of the following data processing activities: (a) collection; (b) alteration; (c) access/consultation; (d) disclosure including transfers; (e) combination; and (f) erasure.

› **7.3 – Data Retention**

Law enforcement authorities should retain data only for an appropriate period.

CHAPTER VIII – SENSITIVE DATA PROCESSING

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.

CHAPTER IX – DATA SUBJECT RIGHTS

The ninth chapter highlights data subjects' right to access and right to rectification or erasure.

› **9.1 – Right to Access. and 9.2 – Right to Rectification or Erasure.**

9.1 – RIGHT TO ACCESS

The right to access provides a data subject with the ability to have direct or indirect access to the data processed about the data subject in the WAPIS.

9.2 – RIGHT TO RECTIFICATION OR ERASURE

The right to rectification or erasure provides a data subject with the ability to request law enforcement authorities to rectify or erase inaccurate personal data pertaining to them that is contained in the WAPIS.

CHAPTER X – DATA PROTECTION IMPACT ASSESSMENT

The tenth chapter discusses the data protection impact assessment, a mechanism that can be used to help law enforcement authorities assess and record risks involved in implementing the WAPIS. A good data protection assessment will evidence that law enforcement authorities considered the risks related to the intended processing and that law enforcement authorities considered their broader data protection obligations.

CHAPTER XI – EXCEPTIONS

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

CHAPTER XII – CONCLUSION

Lastly, 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 sharing and maximize overall use of the WAPIS.

INTERPOL

INTERPOL BUREAU RÉGIONAL ABIDJAN
ANNEXE
RUE E70, À PROXIMITÉ DE L'ÉGLISE
BON PASTEUR
RIVIERA 3 EECI, LOT 1199 ILOT 125
ABIDJAN
CÔTE D'IVOIRE

WWW.INTERPOL.INT

@INTERPOL_HQ WWW.INTERPOL.INT INTERPOLHQ