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.

CHAPTER V

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

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.

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.

CHAPTER VII

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.

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.

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.

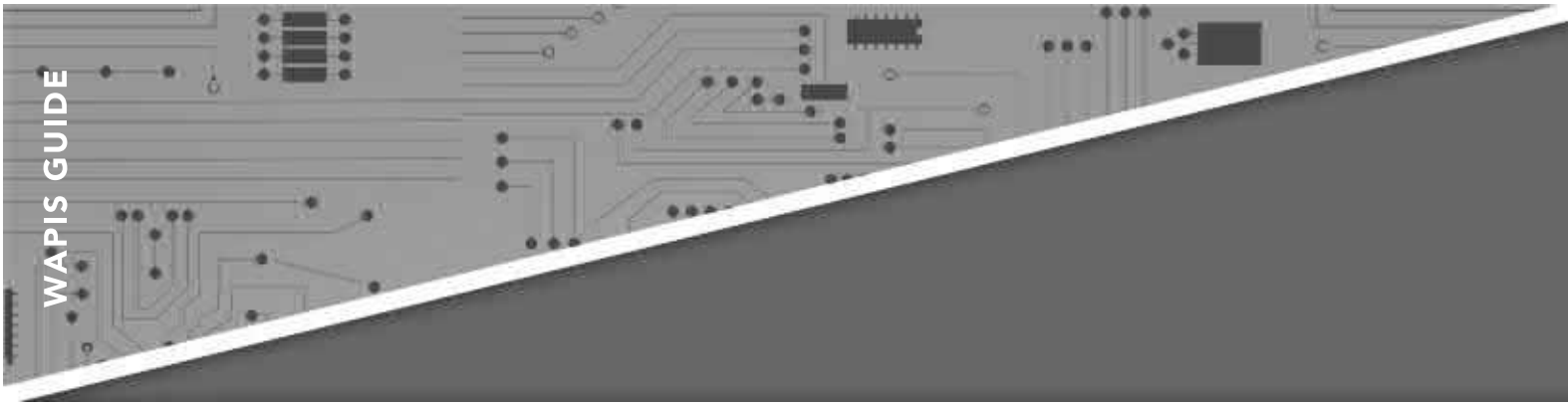
The court agreed that the recording of the word "prostitute" in Ms. Khelili's police file was an interference in accordance with the law for the purpose of preventing disorder and crime and for the protection of the rights of others. While the word "prostitute" as a profession had been deleted from the 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



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.

CHAPTER X

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.

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 XI

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.

CHAPTER XII

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:

› 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

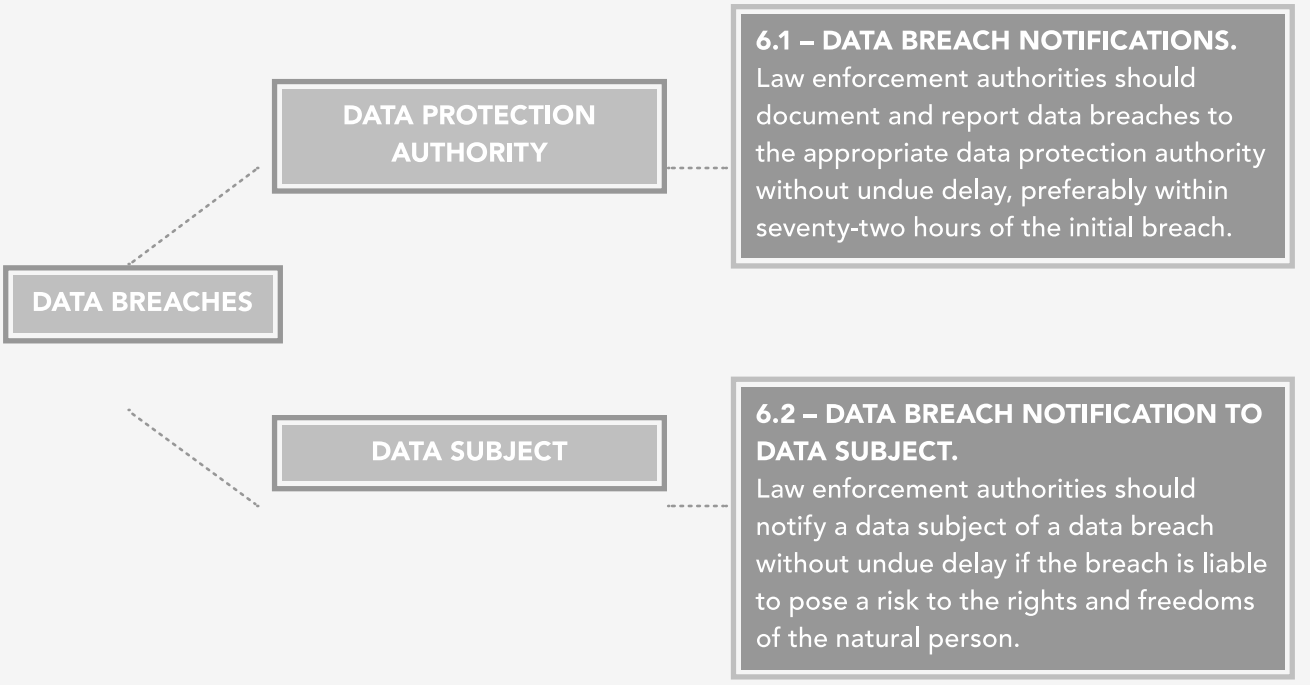
Law enforcement authorities should not share inaccurate, outdated, or incomplete personal data. If inaccurate personal data are shared, law enforcement authorities should notify the recipient without delay and take appropriate steps to rectify, erase or restrict the processing of the data.

› 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

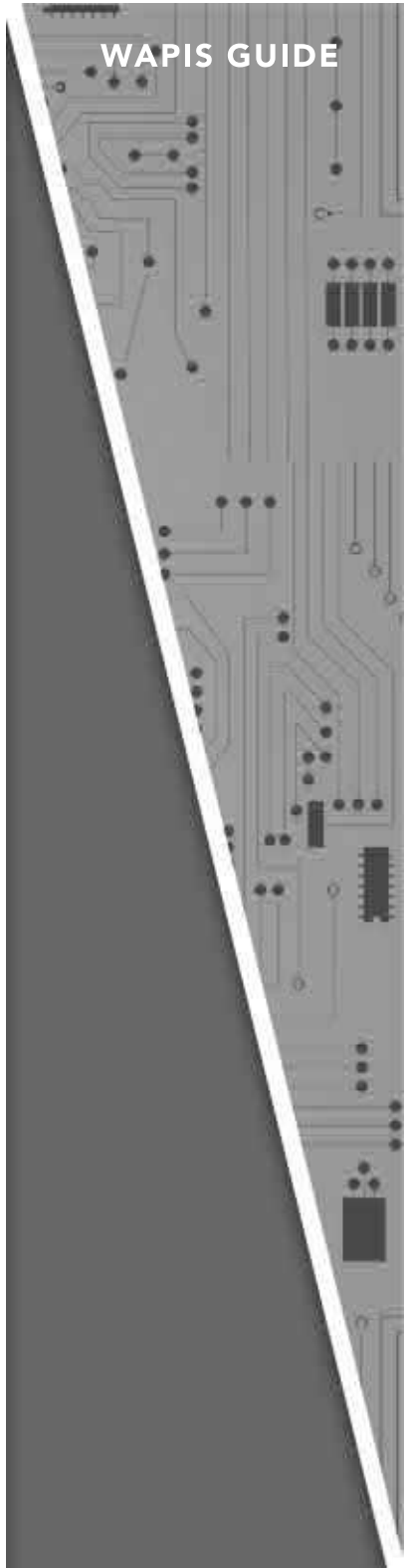
The tenth chapter discusses the data protection impact assessment, a mechanism that can be used to help law enforcement authorities assess and record risks involved in implementing the WAPIS. A good data protection assessment will evidence that law enforcement authorities considered the risks related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

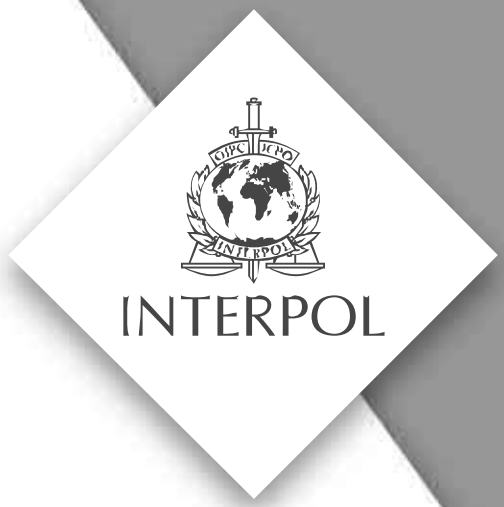
CHAPTER XI – EXCEPTIONS

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.


WAPIS GUIDE



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