سلطنة عمان
وزارة التربية والتعليم

EMC
مسقط 2024
Muscat 2024

إيسيسكو
ICESCO

ICESCO Education Ministers Conference

ICESCO EMC 3

Beyond Transforming Education Summit: from Commitments to Actions

3.5

Digital Education

Muscat, Sultanate of Oman

2-3 October **2024**

سلطنة عمان
وزارة التربية والتعليم

EMC
مسقط 2024
Muscat 2024

إيسيسكو
ICESCO

ICESCO Education Ministers Conference

ICESCO EMC 3

Beyond Transforming Education Summit:
from Commitments → to Actions

3.5

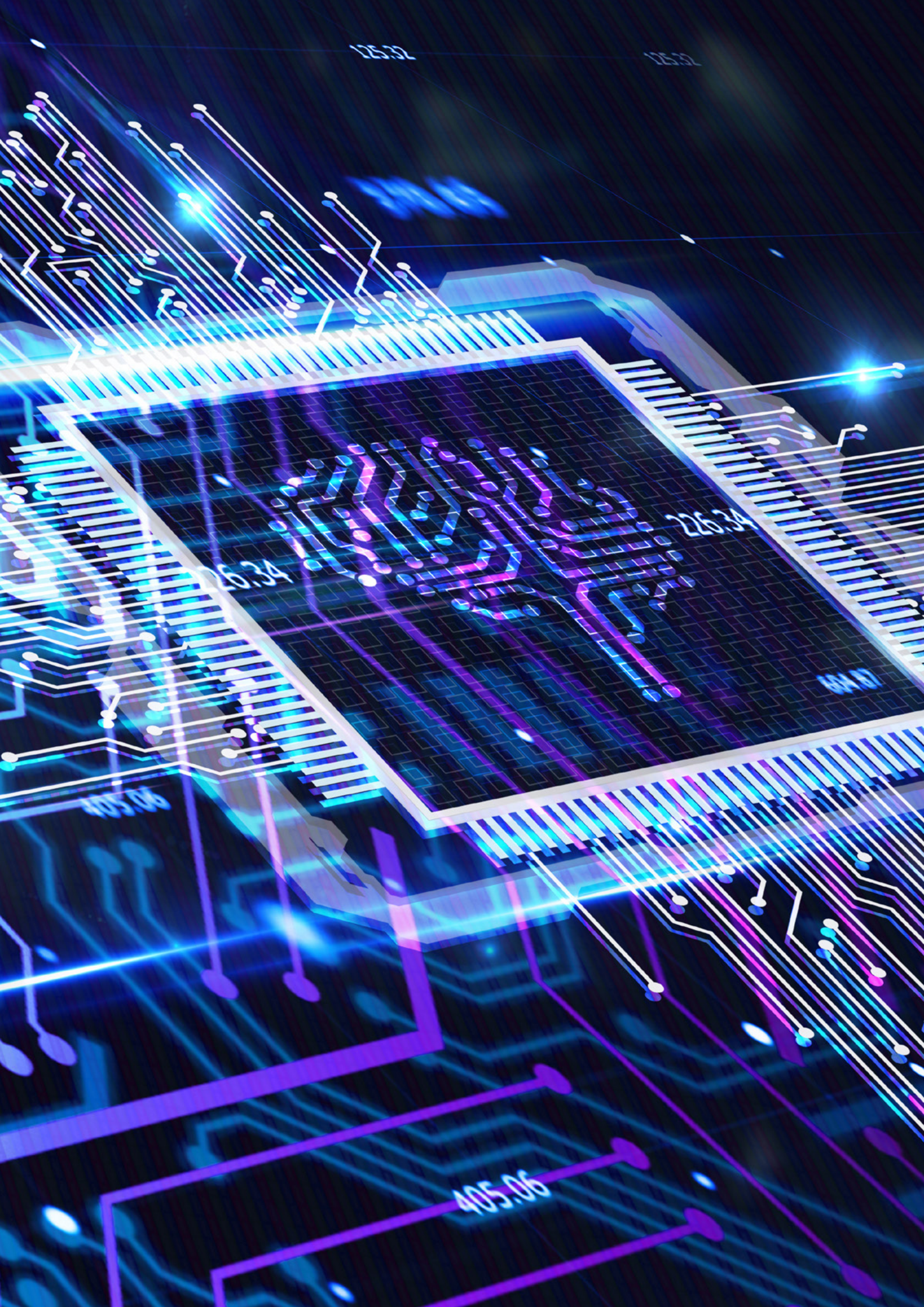
Digital Education

Muscat,
Sultanate of Oman

2-3
October

2024

SUMMARY


125.32
125.32
26.34
26.34
405.06
405.06

0

FOREWORD

A. OBJECTIVES

B. IMPORTANCE OF PERSONAL DATA SECURITY

C. ROLE OF DIGITAL EDUCATION

D. CASES OF ICESCO MEMBER STATES

FOREWORD

With the advent of digital technology and artificial intelligence, humanity is increasingly being surrounded by a digital environment that continues to shape individuals' daily lives in many ways and on various dimensions. Indeed, the opportunities provided by this digital environment, particularly in the field of education, are well documented and proven. However, this environment can trigger a number of risks undermining the well-being of its users and threatening their fundamental human rights. These risks include, among others, the breach and exploitation of personal data.

To this end, policy makers and practitioners, including legislators, supervisory authorities as well as the digital technology industry are called on to promote guidelines and implement measures to fulfill their data protection obligations aimed at safeguarding the privacy of their citizens. The stakeholders concerned need to be aware of this growing problem, and adopt solid data protection measures and guidelines. Such measures should address the need for sound personal data management and protection practices for all entities involved in the processing and use of personal data. They should draw on the standards and principles of international and national laws and policies to foster a culture of personal data protection.

This guide is primarily designed to provide decision-makers with a coherent overview of the importance of promoting the security and confidentiality of personal data in the digital environment. It reviews all the fundamental concepts and texts relating to the protection of personal data, including their collection, storage, processing and sharing, as well as the security measures and risk management policies that can be implemented for data protection. It provides practical guidelines for promoting digital literacy and a culture of data privacy in an increasingly interconnected digital world.

A. Objectives

Furthermore, the key objective of this guide is to raise awareness among decision-makers, researchers, users, citizen organizations and governments of the challenges and issues related to data protection in the current digital environment, by promoting a proactive analysis approach that anticipates and identifies potential risks associated with the growing use of new digital technologies.

In addition, this guide aims to promote a culture of accountability and transparency in personal data management, by encouraging organizations to adopt policies and practices that comply with international standards and current data protection regulations, through the development of cooperation mechanisms and a collaborative framework between stakeholders in ICESCO's Member States, with a view to promoting the exchange of information and best practices, and encouraging collaboration and experience-sharing among actors in the digital environment, thus fostering synergies in the field of data protection, the development of common standards, capacity-building, and compliance with basic data protection standards, etc.

B. Importance of personal data security

In today's intricate ecosystem of the information and communication society, the protection of personal data plays a crucial role on several levels. First and foremost, it is vital to preserving individual privacy in an environment where personal data is exchanged on an unprecedented scale. This protection is essential to ensure that individuals keep control of their information and avoid any form of exploitation.

Moreover, data protection is a fundamental pillar of digital trust. Setting strong security and confidentiality standards fosters a climate of trust between users, businesses and governments, which is essential for promoting the widespread adoption of information and communication technologies (ICTs) and thus stimulating innovation and economic growth.

In addition, amid the rampant global cyber threats, data protection is an essential component of cybersecurity. Thus, the implementation of adequate protection measures helps prevent data breaches and cybercrimes that could compromise the stability and security of the information society.

Data protection is also a key ethical and political issue, raising major questions about the protection of privacy, the promotion of individual freedoms and corporate and governmental social accountability. Ensuring the safe, ethical and responsible use of data helps preserve democratic values and fundamental rights in an ever-changing digital environment.

Personal data protection is an ethical, economic and social code of conduct that requires continuous attention and concerted commitment from all stakeholders.

C. Role of Digital Education

Digital education plays an essential role in promoting the protection of personal data. It makes individuals aware of the confidentiality and security issues involved in handling personal data in a digital environment. Providing people with the necessary knowledge and skills for understanding the fundamental principles of data protection helps them safely navigate in the digital world, while making informed decisions on how to provide, manage and protect their personal information and data.

Digital education introduces young users to the good and best practices of personal data protection.

This involves integrating the concepts of personal data protection and privacy into school curricula to equip learners with skills likely to ensure data security and confidentiality in the digital space.

In addition, digital education on personal data encourages the development of innovative digital solutions to strengthen data protection. Promoting research and innovation in cybersecurity and privacy protection encourages the emergence of new approaches and tools to ensure the security and integrity of personal data in a constantly evolving digital world.

Digital education instills a culture of responsibility and digital citizenship. This is reflected in a two-fold approach: the principle of the right to privacy and data protection for every citizen, and the responsibility of every user to protect his or her own personal data as well as other users' data, whenever possible.

Digital education training and learning will thus create a safer, and a more ethical, inclusive, responsible and equitable online experience for all users.

D. Cases of ICESCO Member States

Privacy is protected as a human right under Article 12 of the Universal Declaration of Human Rights and Article 17 of the International Covenant on Civil and Political Rights.Countries worldwide, including ICESCO Member States, have data protection laws that reinforce the protection of privacy, with over 132 countries having drafted and adopted such laws based on international standards.

The protection of personal data in the Member States of the Islamic World Educational, Scientific and Cultural Organization (ICESCO) has become a growing concern amid the rapid digital transformation in our societies.

Despite the varying levels of development in personal data protection policies, strategies, and systems among Member States, all countries recognize the critical importance of protecting personal data, privacy, and confidentiality in a digital environment. ICESCO Member States have begun to develop legal and regulatory frameworks to ensure the protection of personal data in line with international standards and Islamic principles.

Efforts have been made to promote regional, interregional, and international cooperation in order to reflect on how to address these concerns, and to create dynamics of exchange and collaboration that serve the emergence of healthy and inclusive environments in ICESCO's Member States.

This guide provides a non-exhaustive overview of the legal and organizational efforts made by ICESCO's Member States. These efforts include the enactment of legislation on personal data protection, the development of control mechanisms to ensure compliance with relevant laws and regulations, and the promotion of awareness and training for both professionals and citizens on privacy and data security issues. Such initiatives aim to strengthen their ability to protect personal information in the digital sphere.

1

“PROTECTION OF PERSONAL DATA, LEGAL FRAMEWORK, AND ISSUES FUNDAMENTALS”

A. VARIOUS DEFINITIONS OF PERSONAL DATA

B. PROTECTION OF PERSONAL DATA, LEGAL FRAMEWORK, ISSUES AND FUNDAMENTALS

C. EVOLUTION OF PRACTICES FOR COLLECTING, PROCESSING AND USING PERSONAL DATA

D. PERSONAL DATA PROTECTION ISSUES, RISKS AND DIGITAL TRUST.

A. VARIOUS DEFINITIONS OF PERSONAL DATA

There are various definitions of personal data, depending on the legal and regulatory context. Below are some of the common definitions:

According to Article 4, of the European Union's General Data Protection Regulation (GDPR)[1] "Personal data" means any information relating to an identified or identifiable natural person (hereinafter referred to as a "data subject"); an "identifiable natural person" is deemed to mean a natural person who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, identification number, location data, an on-line identifier or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person. This includes information such as IP address, biometric data, etc.

Canada's Personal Information Protection and Electronic Documents Act (PIPEDA)[2], defines personal data as any information or more detailed information relating to an identifiable individual, namely information about the individual's physical or mental health.

The UK Data Protection Act (DPA) [3] defines personal data as any data that could be used to identify a living individual. Anonymized or aggregated data was less regulated by law, provided that the anonymization or aggregation was not carried out in a reversible manner. This can include data such as name, address, e-mail

address, phone number, medical data, financial data and so forth.

In the United States, the California Consumer Privacy Act (CCPA)[4], similar to other states, defines personal data as any information that relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household. The CCPA guarantees the privacy rights and the protection of consumers residing in California with regard to their personally identifiable information. The CCPA aims to strengthen consumer privacy in California by imposing obligations on companies that collect and process personal data.

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 2016, on the protection of individuals with regard to the processing of personal data and on the free flow of such data, and repealing the Directive 95/46/EC (General Data Protection Regulation.

[2] Canadian Personal Information Protection and Electronic Documents Act (S.C. 2000, c. 5)

[3] DPA: Data Protection Act 2018, the UK's new data protection law, was granted the Royal Seal on May 23, two days before the entry into force date of 2016/679 ("RGPD").

[4] CCPA: California Consumer Privacy Act is the data protection law, aimed at protecting the personally identifiable information (PII) of US California residents, enacted in 2018, effective in 2020

Personal data includes the so-called "sensitive" data category, which refers to information that, due to its nature, once disclosed, may present a major risk to the privacy and physical or moral security of individuals. Such data generally includes information relating to ethnic or racial origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, state of health or sex life. Due to their sensitive nature, such data often requires enhanced protection and is generally subject to stricter restrictions on collection, processing and sharing in accordance with applicable laws and regulations.

Personal data is defined in the countries of the Islamic world in a similar way to its definition in the European Union or other western countries, being personal data or information relating to an identified or identifiable natural person. However, the precise details may vary according to the specific laws of each country.

The various definitions may differ slightly from one legal system to another, but they all share the idea that personal data is information that can be used to identify or link a specific person.

B. PROTECTION OF PERSONAL DATA, LEGAL FRAMEWORK, ISSUES AND

The World Summit on the Information Society (WSIS), held in Tunisia, in November 2005, addressed the issue of data protection in its documents and declarations.The declaration adopted during the first phase of the WSIS, in 2003, stresses the need to build trust and security in the use of ICTs, by promoting the protection of personal data and privacy, as well as the security of transactions. This is essential to ensure the safe and reliable use of information and communication technologies.

This text emphasizes the crucial importance of protecting personal data and privacy in the context of using information and communication technologies (ICT). It also underscores the need to create an environment of trust and security for users.

The foundations of personal data protection are based on a number of essential principles, mainly grouped into six main principles . These include consent and transparency, the definition of purposes, the guarantee of data reliability, the implementation of security and confidentiality measures, and the recognition and exercise of data-related rights.

Consent and transparency: les Individuals must give their clear and explicit consent for their personal data to be collected, processed or shared, so organizations, or any legal or natural person, are required to be transparent about how they use personal data and to provide clear and understandable information about the purpose and collection, processing and confidentiality of personal data.

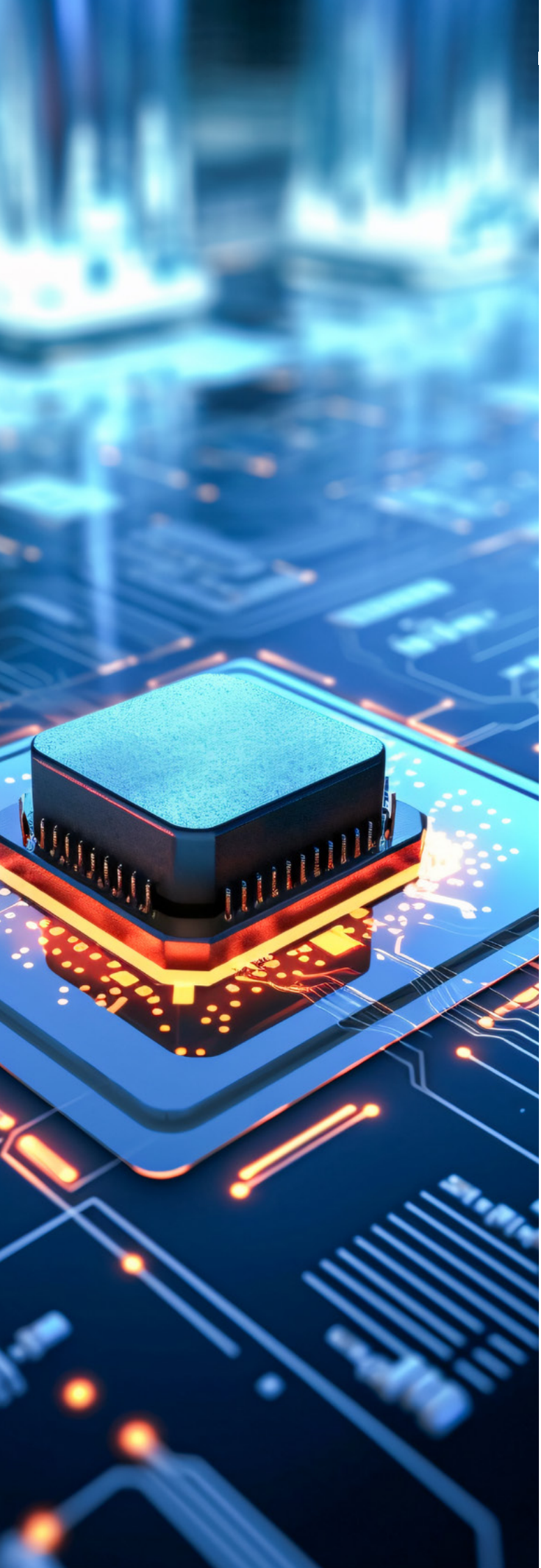
Purpose of data collection and processing: Personal data must only be collected and processed for a specific and legitimate purpose, and must not be used subsequently in a way that is incompatible with these initial purposes. Organizations are therefore required to limit data collection to the minimum necessary to achieve the specified purposes. This means collecting only data that is relevant and proportionate to the purposes of the processing.

Data accuracy: Organizations are responsible for ensuring that the personal data they hold is accurate, complete and up-to-date.

Security and confidentiality: Organizations collecting and processing personal data are responsible for implementing all appropriate security measures to protect personal data against loss, unauthorized access, disclosure or destruction. This includes practices such as data encryption or database access management.

Respecting individual rights: Individuals enjoy certain rights relating to their personal data, including the right to access their data, to correct it if inaccurate, to delete it, to object to its processing, or to request portability to another service provider.

[5] CNIL, August 23, 2019, the six main principles of the General Data Protection Regulation (GDPR), adopted on May 24, 2016 by the European Parliament and the Council. DPA: Data Protection Act 2018, h



By adhering to these fundamental principles, organizations can ensure the adequate protection of personal data while respecting individuals' rights and privacy expectations.

Compliance with the principles of personal data protection is part of the missions of the data controller, which is defined as an entity or individual responsible for determining the purposes and methods of data processing, and who is responsible for ensuring that data processing is carried out in compliance with current laws and regulations. The data controller may be a company, a public organization or any other entity that collects, uses or stores personal data. They are also responsible for guaranteeing the security and confidentiality of the data, as well as respecting the data protection rights of individuals. In the event of non-compliance, the data controller may be subject to sanctions and fines.

Artificial intelligence (AI) has significantly transformed the collection, processing, and use of personal data. Thanks to AI, companies can automate and optimize these processes, offering increased personalization of services and more sophisticated data analysis. However, this also raises concerns about privacy and data security, requiring appropriate regulation and oversight.

C. EVOLUTION OF PRACTICES FOR COLLECTING, PROCESSING AND USING PERSONAL DATA

Since the 2000s, when social networks were launched, practices for collecting, processing and using personal data have changed radically with the rise of digital technologies. Data used to be collected for simple transactions: in the commercial sector, it was used to register customers so that purchases could be delivered, invoices sent... What used to be simple data collection for specific transactions was transformed, around 2010, into a much more complex process. Today, data is collected from multiple sources, including social networks, connected objects and mobile applications, capturing information about people's habits, preferences and behaviour.

The processing of this data now relies on advanced technologies such as Big Data and artificial intelligence. Big Data enables huge volumes of data to be analysed in real time, providing invaluable insights for decision-making and personalising services. Artificial intelligence, for its part, facilitates complex tasks such as pattern recognition, behaviour prediction and adapting offers to users' needs.

However, this technological advance poses major challenges for the protection of privacy. The expansion of data collection and analysis increases the risks of surveillance, profiling and misuse of personal information. Hence the role of digital education in raising people's awareness of how to manage their data in order to limit these risks. With this in mind, there is a need for stricter regulations to govern the use of data and ensure an ethical and secure approach, thereby protecting users' privacy.

D. PERSONAL DATA PROTECTION ISSUES, RISKS AND DIGITAL TRUST

The concept of digital trust is centered on creating a safer digital environment for online interactions by promoting the protection of personal data and ensuring the confidentiality of individuals and organizations. It also encompasses the security, confidentiality, and integrity of data in the digital world. Legally, digital trust is defined by the rules and standards that ensure this protection, including data protection legislation and comprehensive cybersecurity measures and standards [6], [7].

When individuals provide their personal information online, they expect it to be treated securely and confidentially in accordance with the purpose for which it is collected, based on their prior consent. However, privacy and data security risks can compromise this trust.

Cybercrime, cyberattacks, data breaches and abusive data collection and processing practices can have harmful consequences for individuals, ranging from identity theft to disclosure of sensitive data or data leakage. These incidents, or even crimes, not only infringe on users' privacy but also undermine trust in the companies and institutions responsible for protecting this data.

To promote digital trust, it is essential to implement effective data protection measures [8], such as encryption technologies and the management of database access authorizations, as well as raising users' awareness of good cybersecurity practices and the protection of their personal data.

The security and confidentiality of personal data is an essential component in strengthening people's confidence in the digital ecosystem, and in fostering a safer online environment.

[6] LoiLaw No. 2004-575 of June 21, 2004, on trust in the digital economy (France)

[7] Personal Information Protection and Electronic Documents Act (PIPEDA) (Canada)

[8] Law No. 43-20 on trust services for electronic transactions (Morocco)

2

“INSTITUTIONAL AND ORGANIZATIONAL STRENGTHENING FOR THE PROTECTION OF PERSONAL DATA”

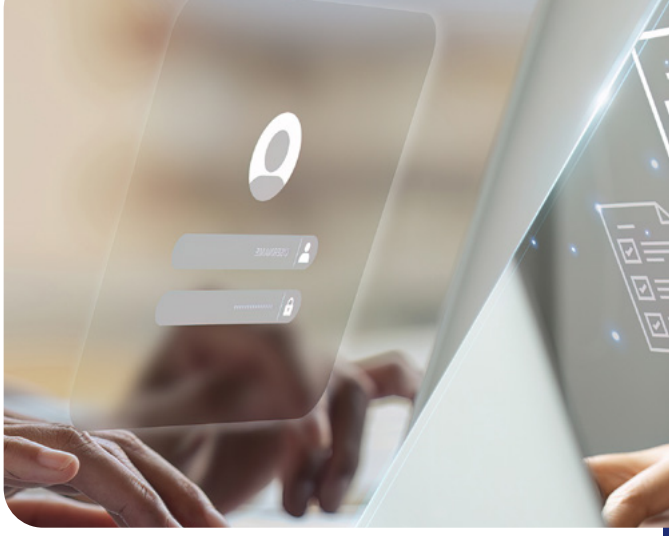
A. ROLE AND MISSION OF THE DATA PROTECTION AUTHORITY.

B. INTERNAL LEGAL COMPLIANCE POLICIES FOR A GIVEN ORGANIZATION.

C. TRAINING ON BEST PRACTICES FOR STAFF RESPONSIBLE FOR PROCESSING AND MANAGING PERSONAL DATA.

D. ADOPTION OF SECURE TECHNOLOGIES FOR PERSONAL DATA PROCESSING.


AI
10 1001 01010 10
0 11 0010
10



A. ROLE AND MISSION OF THE DATA PROTECTION AUTHORITY

The personal data protection authority is an independent government body tasked with protecting personal data within a country or region. Its primary role is to ensure compliance with data protection laws and regulations by overseeing and regulating data processing activities. It acts as a monitoring body, enforcing compliance with personal data protection laws and ensuring compliance. The authority is also responsible for investigating potential breaches and can impose sanctions for non-compliance. As a supervisory body, it enforces compliance with personal data protection laws. It is also responsible for investigating potential breaches and can impose sanctions for non-compliance. Additionally, it offers support and guidance to companies and individuals on best practices for data protection and plays a key role in raising public awareness about privacy and data security issues.

In the context of a connected digital world, the personal data protection authority collaborates with national security and cybersecurity authorities, as well as other data protection authorities internationally, to promote cooperation and harmonization of data protection standards.

B. INTERNAL LEGAL COMPLIANCE POLICIES FOR A GIVEN ORGANIZATION

In any organization, corporate or otherwise, adopting internal policies for compliance with legal standards and regulations for the protection of personal data is crucial. These policies ensure adherence to data protection principles, which are key to building digital trust and respecting privacy. Such a policy includes clear procedures and guidelines to guide the different cycles of data protection - collection, processing, and storage - ensuring that they comply with current laws and regulations. Appointing a Data Protection Officer (DPO) is essential to monitor and supervise compliance with data protection standards.

In all Member States of the European Union (EU), in accordance with the General Data Protection Regulation (GDPR), all companies handling personal data are required to appoint a Data Protection Officer (DPO).

To comply fully with data protection standards and keep pace with technological and legal developments, organizations should establish ongoing training programs. These programs aim to reinforce the skills of responsible staff and raise awareness of good data protection practices and the risks associated with privacy breaches.

The organization should also implement technical measures, digital infrastructures, and appropriate governance to guarantee the security and confidentiality of personal data. This includes data encryption technologies, database access management, and general cybersecurity measures. Regular internal audits should be conducted to assess compliance with legal data protection standards and make necessary adjustments.

C. TRAINING ON BEST PRACTICES FOR STAFF IN CHARGE OF PROCESSING AND MANAGING PERSONAL DATA

Strengthening an organization's capacity in personal data protection requires implementing a training program on best practices for staff responsible for processing and managing personal data. This program should also involve all other staff. Identifying specific training needs in advance, based on roles and responsibilities, is crucial.

The training program should include materials that highlight the principles and foundations of data protection, legal and regulatory obligations, the risks associated with privacy breaches, and the security measures to be adopted. To ensure staff commitment, the program should be interactive and inclusive, featuring practical workshops and case studies. Qualified trainers or experts should be used, alongside appropriate resources and tools. Regular awareness-raising sessions are crucial to reinforce good practices and data protection obligations.

Implementing a mechanism to measure the effectiveness of the training program through continuous evaluations is also advisable. This allows for ongoing adjustments to ensure compliance with data protection standards.

For example, to support companies in complying with the General Data Protection Regulation (GDPR), France's CNIL has created an online training program. Aimed at current and future Data Protection Officers (DPOs) as well as professionals wishing to familiarize themselves with the GDPR, this program consists of training workshops in the form of MOOCs accessible to all. These workshops include videos, texts, illustrations, practical cases, quizzes, and assessments. The four main modules cover the key concepts of the GDPR:

Module 1: GPDR and its key concepts

Module 2: Data protection principles

Module 3: The responsibilities of stakeholders

Module 4: DPOs and compliance tools

Training is free and open to all. At the end of each module, a certificate is issued to participants who complete the course.

[9] CNIL (France) GPDR training workshops (MOOC)
https://www.cnil.fr/fr/comprendre-le-rgpd/le-mooc-de-la-cnil-est-de-retour-dans-une-nouvelle-version-enrichie

D. ADOPTION OF SECURE TECHNOLOGIES FOR PERSONAL DATA PROCESSING

Processing personal data, especially sensitive data, requires a specific approach to ensure security. Robust technical protection systems must be adopted, particularly encryption technologies based on strong cryptographic algorithms..

For Example:

AES (Advanced Encryption Standard): one of the most widely used symmetrical encryption algorithms, approved by the US government to protect sensitive information.

RSA (Rivest-Shamir-Adleman): an asymmetric encryption algorithm widely used for Internet communication security. RSA uses a key pair (public and private) to encrypt and decrypt data, offering robust security for personal data.

ECC (Elliptic Curve Cryptography): an asymmetric encryption algorithm, well suited to protecting personal data on mobile devices and embedded systems.

These and other encryption technologies are essential to protect personal data during processing, transmission and storage.

Additionally, using firewalls and antivirus software can help prevent cyber-attacks and security breaches.

Enhanced security also involves multi-factor authentication solutions, which require several forms of identification before accessing data. Identity and access management tools can be used to control and limit access to data according to user roles and permissions.

3

“DIGITAL EDUCATION AND PROTECTION OF PERSONAL DATA”

A. DIGITAL EDUCATION AND PERSONAL DATA

B. IMPLEMENTING EDUCATIONAL AND COMMUNICATION PROGRAMS

C. BEST PRACTICES FOR THE SAFE USE OF DIGITAL TECHNOLOGIES

D. RAISING AWARENESS AND INDIVIDUAL AND COLLECTIVE RESPONSIBILITY

A. DIGITAL EDUCATION AND PERSONAL DATA

Digital education and personal data protection are closely linked, and are of crucial importance in an increasingly connected and digitized world. Digital education raises awareness about personal data protection challenges among users of all ages, from children to senior citizens. It helps them understand the various risks associated with the disclosure of personal information online, and equips them with the knowledge they need to protect themselves from these dangers.

Additionally, a solid digital education enables individuals to develop the skills needed to protect their personal data. By learning good and best practices for confidentiality and privacy on online platforms, recognizing the various facets of cybercrime, and understanding attack vectors such as phishing and identity theft, individuals can adopt appropriate data security practices.

Introducing digital education from an early age and integrating data protection concepts and best practices into educational curricula will be of great importance in promoting a culture of privacy and data security.This is vital for preventing privacy breaches and strengthening trust in the digital environment.

Moreover, effective digital education can play a key role in raising awareness of individuals' data protection rights and the responsibility of data controllers in organizations. It helps promote the ethical and responsible use of technology.

Ultimately, digital education and data protection are complementary and mutually reinforcing, fostering a safer, more secure and privacy-friendly digital environment.

B. IMPLEMENTING EDUCATIONAL AND COMMUNICATION PROGRAMS

The implementation of educational and communication programs, such as Media and Information Education (MIE) focused on the protection of personal data, is crucial in establishing digital literacy and reinforcing individuals' understanding of the potential risks associated with the disclosure of personal information online and offline. These programs aim to develop an understanding of their rights, responsibilities and the importance of protecting their privacy.

Designed to inform, raise awareness, and educate individuals about the importance of personal data protection, these programs also teach best practices to ensure online security. They can take various forms depending on the context and target audience, including interactive seminars, hands-on workshops, online or offline awareness campaigns, courses, or educational materials.

For example, Scandinavian countries, known for their excellent educational systems, have integrated programs to raise awareness about personal data protection. Norway, for instance, considers education fundamental to society and has implemented educational policies to train citizens on personal data protection.

In Norway, students are introduced to online privacy principles, the risks associated with sharing personal information, and best practices for protecting privacy. They learn about their rights as Internet users, manage privacy settings on online platforms, interpret terms of service, and exercise their rights over personal data. Norwegian teachers receive training on data protection awareness, enabling them to impart this knowledge to students and guide responsible Internet use. Schools also encourage parental involvement through workshops and informational sessions.

Educational programs should be age-appropriate and tailored to students' needs, providing practical and clear advice on protecting personal data. It's important to emphasize technical and legal aspects to develop skills in managing privacy settings, securing passwords, recognizing phishing attempts, protecting against malware, and understanding data protection regulations. This includes explaining rights such as consent, access to collected personal information, and the right to object or rectify.

Effective communication approaches are crucial for spreading digital culture centered around privacy rights and personal data protection. This encourages collective awareness and responsible technology use.

C. BEST PRACTICES FOR THE SAFE USE OF DIGITAL TECHNOLOGIES

To better protect personal data in the digital environment, it is essential for users of new technologies to develop vigilant online behaviors. Various training programs will enable users to adopt responsible behaviors based on adherence to a non-exhaustive list of basic cybersecurity best practices, such as:

- **Using strong and unique passwords for each online account:** Create passwords that are a combination of letters, numbers, and special characters.
- **Enabling two-factor authentication whenever possible:** This adds an extra layer of security to accounts on social networks, email accounts, or online games, for instance.
- **Minimizing shared personal information online:** Share personal data only when necessary, ensuring that the websites are trustworthy and secure, and adjusting privacy settings on online platforms.
- Installing antivirus software and firewalls: Protect devices from malware, spyware, and online threats.
- **Regularly updating software, applications, and operating systems:** Benefit from the latest security patches to address potential vulnerabilities.
- **Being cautious of unsecured links or attachments coming from untrusted or unknown sources:** Protect against phishing attacks designed to steal personal or sensitive data.
- **Being wary of connections to unsecured public Wi-Fi networks:** Especially avoid carrying out sensitive transactions or accessing personal accounts.
- **Staying alert to fraud or identity theft attempts:** Verify the authenticity of communications and report any suspicious behavior.

The rapid advancement of digital technologies has significantly increased risks, particularly with the proliferation of connected devices, the widespread adoption of artificial intelligence, and the advent of the Metaverse. In this context, it is imperative to increase our vigilance to ensure secure navigation. This requires adopting appropriate practices, such as:

- **Researching connected devices (smartwatches, home automation, cameras, etc.):** Understand their features, functionality, and interactions with other electronic devices. Connected devices still have security flaws in terms of personal data protection.
- **Protecting sensitive personal data used by AI systems:** Implement robust security protocols, such as encryption, pseudonymization, and access management. It is crucial to ensure that sensitive data processed by AI is secure and compliant with regulations in effect.
- **Establishing continuous monitoring mechanisms:** Detect anomalies and deviations in the behavior of AI systems in production, and respond quickly to identified issues to prevent harmful consequences.
- **Remaining vigilant against new phishing techniques powered by artificial intelligence:** These sophisticated attacks can use AI algorithms to personalize messages and bypass traditional defenses, highlighting the importance of vigilance and awareness to prevent such fraud.

D. RAISING AWARENESS AND INDIVIDUAL AND COLLECTIVE RESPONSIBILITY

Raising awareness about personal data protection in the digital environment is essential, especially as personal information becomes more vulnerable to online threats with advancements in digital technologies, particularly AI applications. Awareness helps individuals understand the risks associated with disclosing personal information online and emphasizes the importance of maintaining privacy.

Protecting personal data is a shared responsibility between individuals and various stakeholders, including society as a whole. Individuals must take measures to protect their personal data by adopting good online security practices and understanding legal and regulatory aspects. Society collectively promotes a culture of personal data protection, emphasizing awareness and education about image rights on digital platforms and social networks. This effort should involve the entire educational community, including parents, guardians, and teachers, who play a crucial role in this endeavor.

[10] Law No. 2024-120 of 19 February 2024 (France)

4

“PROTECTION OF PERSONAL DATA IN ICESCO MEMBER STATES”

A. NATIONAL AND INTERNATIONAL REGULATIONS ON PERSONAL DATA PROTECTION

B. COMPARATIVE ANALYSIS OF NATIONAL LEGISLATION IN ICESCO MEMBER STATES

C. CHALLENGES IN HARMONIZING REGULATIONS AND PRACTICES

D. CHALLENGES IN IMPLEMENTING AWARENESS AND CAPACITY-BUILDING STRATEGIES


Card Purchased
Wallet Recharge
Search
Finance business

A. NATIONAL AND INTERNATIONAL REGULATIONS ON PERSONAL DATA PROTECTION

National and international regulations on personal data protection play a crucial role in safeguarding individuals' privacy and security in a rapidly evolving digital landscape. Initial international concerns about data protection and privacy, which laid the groundwork for recent regulations in response to technological advances, emerged in the 1970s.

Over the decades, several key milestones have been achieved, including the adoption of significant laws and regulations such as the Privacy Act in the United States (1980s), the Council of Europe's Convention 108 (1981), and the EU's General Data Protection Regulation (GDPR) (2016). These regulations aim to protect individuals' fundamental rights in an increasingly digital world.

Various international organizations, such as the United Nations, the Organization for Economic Cooperation and Development (OECD), and the Council of Europe, have developed instruments and recommendations to promote uniform personal data protection globally. Key instruments include the Universal Declaration of Human Rights (1948), the Council of Europe Convention 108 (1981), the EU Data Protection Directive (1995), and the GDPR (2018).

At the national level, many countries have adopted specific data protection laws, such as the Personal Data Protection Law (PDPL) in South Korea, and the California Consumer Privacy Act (CCPA) in the United States. These laws establish strict standards and requirements for collecting, processing, and storing personal data, along with mechanisms for enforcing these rules and sanctioning violations.

These national and international regulations create a legal framework to ensure personal data is processed ethically, securely, and in accordance with fundamental rights. They also encourage cooperation among countries to address cross-border data protection challenges, such as international data transfers and combating cybercrime. By promoting a harmonized approach to data protection, these regulations enhance digital trust and uphold privacy as a fundamental right.

B. COMPARATIVE ANALYSIS OF NATIONAL LEGISLATIONS IN ICESCO MEMBER STATES

Some of ICESCO Member States have adopted various approaches to personal data protection, reflecting each country's unique cultural, political, and legal factors. While most Member States have implemented advanced and stringent data protection laws, others are still in the process of developing their regulatory frameworks.

The comparative analysis provided in this guide offers an initial overview of the progress and an understanding of the similarities and differences between national legislations concerning the definition of personal data, individual rights, organizational responsibilities, monitoring mechanisms, and sanctions for non-compliance.

For example, some countries emphasize protecting sensitive data, such as biometric or medical data, while others focus on financial or commercial data. This analysis could also explore how ICESCO Member States address emerging data protection challenges, such as regulating artificial intelligence and the Internet. It might examine concerns like managing biometric data, protection against cyberattacks, and algorithm transparency, revealing strategies for ensuring security and confidentiality in the digital landscape.

An overview of the legal and regulatory framework in ICESCO Member States highlights a diversity of strategies and approaches. It underscores the importance of inter-regional and international cooperation to address common challenges in data protection.

A comprehensive comparative analysis of the data protection laws adopted by ICESCO Member States is essential to identify potential divergences. These differences can pose challenges for collaboration and coherence among national regulatory frameworks. By establishing common standards, Member States can work together to address shared data protection challenges in a globalized digital environment.

The summary table in this guide provides an overview of the landscape of national legislations concerning personal data protection in select ICESCO Member States.

	Member State	Legal Reference	Competent Body
1	Kingdom of Morocco	Law 09-08 on the protection of individuals regarding to the processing of personal data	National Commission for the Monitoring of Personal Data Protection (CNDP)
2	Islamic Republic of Mauritania	Law No. 2017- 020 of July on the protection of personal data	Personal Data protection Authority (APDCP)
3	Republic of Niger	Law No. 2023-31 of 4 July 2023, amending Law No. 2022-59 of 16 December 2022, on the protection of personal data, and Law No. 2022-59 of 16 December 2022, on the protection of personal data	High Authority for the Protection of Personal Data (HAPDP)
4	Federal Republic of Nigeria	Nigeria Data Protection Act (promulgated in 2023)	Nigerian Data Protection Commission (NDPC)
5	Republic of Yemen	None	None
6	Republic of Benin	The data protection protocol in Benin is governed by two legislative texts: Law No. 2017-20 of 20 April 2018, on cyber law, and Law No. 2009-09 of 22 May 2009, dealing with the protection of personal data.	The Beninese data protection authority.
7	Republic of Côte d'Ivoire	Law 2013-450 on the protection of personal data.	Telecommunications and ICT Regulatory Authority of Côte d'Ivoire.
8	State of Kuwait	Decision No. 42 of 2021 on the regulation of data confidentiality protection	Communication and Information Technology Regulatory Authority CITRA
9	Lebanese Republic	Law No. 81-2018	Ministry of Economy and Trade
10	State of Libya	Constitution of 2011, Articles 12 and 13	----

11	Republic of Maldives	No specific law	None
12	Republic of Mali	Law No. 2013-015	Personal Data Protection Authority
13	Malaysia	Personal Data Protection Act 2010 (PDPA)	Personal Data Protection Department
14	Arab Republic of Egypt	Law No. 151 of 2020 on the protection of personal data	National Authority for the Protection of Personal Data
15	Republic of Guinea	Law 37/2016 on cybersecurity and the protection of personal data	Cybersecurity authority ANSSI
16	State of Palestine	None	None
17	Republic of Kazakhstan	Law No. 94-V of 21 May 2013	Ministry of Digital Development, Innovations and Aerospace Industry
18	State of Qatar	Law No. 13 of 2016 on the protection of personal data	National Cyber Governance and Assurance Affairs (NCGAA)
19	Union of the Comoros	None	None
20	Kyrgyz Republic	Law No. 58 of 14 April 2008	State Agency for Personal Data Protection.
21	Republic of Cameroon	Law No. 2010/013 of 21 December 2010, as amended and supplemented by Law No. 2015/06 of 20 April 2015, governing electronic communications in Cameroon.	Telecommunications Regulatory Authority
22	Republic of Sierra Leone	None	None
23	Republic of Senegal	Law No. 2008-12 of 25 January 2008	Commission for the Protection of Personal Data

24	Federal Republic of Somalia	Law No. 005 of 2023	Data Protection Authority
25	Republic of Iraq	None	None
26	Sultanate of Oman	Royal Decree No. 6 of 2022	None
27	Gabonese Republic	Act No. 025/2023 of 9 July 2023, amending Law No. 001/2011 of September 2011 25	The Authority for the Protection of Personal Data and Privacy APDPVP
28	Republic of the Gambia	Ongoing bill	None
29	Co-operative Republic of Guyana	Law No. 18 of 2023 on the protection of personal data	Data Protection Commissionier
30	Republic of Tunisia	Law No. 2019-014 of 29 October 2019	Instance de Protection des Données à Caractère Personnel (IPDCP)
31	People's Democratic Republic of Algeria	Organic Law No. 63469 – 2004, Decree No. 3003470 – 2007	National Authority for the Protection of Personal Data (INPDP)
32	Republic of Djibouti	Ongoing bill	None
33	Kingdom of Saudi Arabia	Royal Decree No. M/19 of 9/2/1443H (corresponding to 16 September 2021), as amended by Royal Decree No. M/148 of 5/9/1444H (corresponding to 27 March 2023)	Saudi Authority for Data and Artificial Intelligence (SDAIA)
34	Republic of the Sudan	None	None
35	Republic of Suriname	Ongoing bill	None
36	Syrian Arab Republic	None	None

37	Islamic Republic of Pakistan	Ongoing bill	None
38	Kingdom of Bahrain	Law No. 30 of 2018, entered into force on 1 August 2019 (Personal data protection law)	Ministry of Justice, Islamic Affairs and Endowments
39	Brunei Darussalam	Personal Data Protection Bill 2021	Authority for Info-communications Technology Industry
40	People's Republic of Bangladesh	No specific law, 2023 Cybersecurity Law	Cybersecurity Agency
41	Republic of Benin	Law No. 2017-20, Law No. 2009-09	Personal Data Protection Authority (APDP)
42	Burkina Faso	Law No. 010-2004/AN	Commission on Information Technology and Liberties (CIL)
43	Republic of Tajikistan	Law No. 1537 of 3 August 2018, Law No. 631 of 15 May 2002, on data protection	Communication Service under the Government of the Republic of Tajikistan
44	Republic of Chad	Law No. 007/PR/2015 governing data protection	The National Agency for Computer Security and eCertification (ANSICE)
45	Islamic Republic of Iran	No specific law	None
46	Republic of Uganda	Law No. 9 of 2019 on data protection and privacy	Personal Data Protection Office under the National Information Technology Authority
47	Hashemite Kingdom of Jordan	Law No. 24/2023 on data protection	None

48	Republic of Uzbekistan	Law No. ZRU-547 on personal data	the Personalization Agency under the Ministry of Justice
49	Republic of Indonesia	Ongoing bill	None
50	United Arab Emirates	Federal Decree-Law No. 45 of 2021 on personal data protection	Office of Data Protection (ODP)
51	Islamic Republic of Afghanistan	None	None
52	Republic of Azerbaijan	No. 998-IIIQ of 11 May 2010, on personal data	Ministry of Transport, Communications, and High Technologies

C. CHALLENGES IN HARMONIZING REGULATIONS AND PRACTICES

Harmonizing international regulations and best practices in personal data protection is crucial, as it promotes consistency across jurisdictions worldwide, enabling compliance for businesses and organizations operating internationally. It also ensures high standards of transparency and security for globally circulating data and facilitates international cooperation in combating cross-border threats such as cybercrime.

The harmonization of regulations faces significant practical challenges due to the cultural, political, and legal differences among countries. These differences make it difficult to draw up regional or universal standards and rules. Indeed, each country has its own specific features, approach to data protection and legal system, making the implementation of internationally harmonized regulations a complex task.

This adds to the constantly evolving technological landscape, introducing additional challenges. Indeed, technological disparities such as artificial intelligence, the Internet of Things (IoT), and blockchain are creating imbalances in the collection, processing, and handling of personal data. These imbalances call for agile and adaptable regulation. Furthermore, international companies and organizations encounter numerous compliance issues due to the varying laws of different countries.

Currently, the growing risks of personal data breaches and privacy invasions emphasize the need for more unified regulations across countries. For instance, European Union countries have adopted GDPR to address the challenges of regulatory diversity and make it easier for data to flow freely within the EU.

To address the challenges mentioned, it is becoming crucial to align regulations and data protection practices across countries. This alignment not only ensures the protection of individuals' fundamental rights in a global digital environment but also promotes the free flow of data worldwide and facilitates international business and cross-border collaboration. Achieving this goal requires close cooperation among governments, international organizations, businesses, and civil society to develop common standards and principles and restore trust and transparency in handling personal data on both regional and global scales, especially among countries with shared cultures or references.

D. CHALLENGES IN IMPLEMENTING AWARENESS AND CAPACITY-BUILDING STRATEGIES

The implementation of a data protection awareness and training strategy faces several practical challenges, mainly the difficulty of fostering widespread awareness among the public, many of whom may not fully recognize the risks associated with disclosing their personal data. Additionally, it is crucial to address the diverse needs and varying levels of understanding across different groups of the population. Awareness-raising and capacity-building programs must be tailored to cater to various audiences, including professionals, young users, and children. This necessitates the development of effective strategies specifically designed to meet the unique characteristics of each target group.

To keep pace with changes in technologies and personal data protection practices, the contents and teaching approaches need to be constantly updated. On the other hand, the disengagement of specific target audiences from awareness-raising programs undermines the long-term impact and effectiveness of the training. Moreover, the implementation of awareness-raising and training strategies requires both financial resources and trained human resources, which can be obstacles to the implementation of comprehensive, long-term, high-quality awareness-raising and training programs.

Setting up mechanisms to evaluate awareness-raising or training strategies is an essential step in measuring the impact of programs, assessing their effectiveness and making the necessary adjustments to constantly improve the strategy of protecting personal data on the internet.

5

“PROTECTION OF PERSONAL DATA AND STRENGTHENING COOPERATION AMONG ICESCO MEMBER STATES”

A. MODELS OF SUCCESSFUL COOPERATION MECHANISMS.

B. DEVELOPMENT OF BASIC STANDARDS AND COMPLIANCE.

C. COOPERATION AND CAPACITY-BUILDING MECHANISMS IN ICESCO MEMBER STATES.

A. MODELS OF SUCCESSFUL COOPERATION MECHANISMS

International cooperation for the protection of personal data is essential to guarantee a consistent and high level of protection on an international scale, thus reinforcing individuals' trust in the use of digital technologies. It also facilitates the exchange of information and best practices among data protection bodies, thereby strengthening their ability to respond to growing data protection challenges. Moreover, it promotes consistency in data protection standards and regulations, reducing obstacles to international development and facilitating the cross-border transfer of data while guaranteeing respect for fundamental privacy rights.

Being aware of the many advantages of such international cooperation, several countries have opted to set up international or regional instruments and conventions:

For instance, the Council of Europe's Conventions 108 and 108+ are the first legally binding instruments on data protection at the international level. The convention provides a framework for cooperation between the Council of Europe's Member States on personal data protection and encourages the adoption of common data protection standards for all countries outside the European Union.

Moreover, The EU-Japan personal data protection cooperation agreement aims to facilitate the transfer of personal data between the EU and Japan by recognizing each party's data protection systems as adequate. This agreement enables companies to transfer data securely without the need for additional guarantee mechanisms.

For its part, The Working Party on Data Governance and Privacy in the Digital Economy (DGP) of the Organization for Economic Co-operation and Development (OECD) brings together representatives of governments and international organizations to discuss emerging data protection challenges and develop guidelines and recommendations for national policies.

Regional Data Protection Networks: These are mechanisms set up by a number of countries to facilitate cooperation and information exchange among data protection bodies on a regional scale, providing a forum for sharing best practices, coordinating cross-border investigations and promoting the convergence of data protection standards, such as the Network of African Data Protection Authorities (NADPA/RAPDP), the Association of Southeast Asian Nations (ASEAN) or the Ibero-American Data Protection Network (IDPN).

A non-exhaustive comparative analysis could also highlight initiatives for cooperation and harmonization of national legislation among ICESCO Member States aimed at strengthening personal data protection on a regional or international scale. This could include information-sharing agreements, technical assistance programs and cooperation mechanisms.

B. DEVELOPMENT OF BASIC STANDARDS AND COMPLIANCE

With the spread of digital services and the increase in data flow across borders, it is imperative to establish common standards and create a coherent, harmonized framework for internationally recognized data protection. Developing these common core standards and ensuring data protection compliance is crucial and brings significant advantages.

Common standards simplify the understanding and application of data protection rules for organizations, businesses, and competent bodies. They also enhance individuals' confidence in the way their personal data is processed, ensuring a uniformly high level of protection regardless of the processing location. Furthermore, adherence to personal data protection standards bolsters the credibility and digital reputation of organizations and companies, fostering improved relations with individuals and partners and building trust in digital services.

Finally, an international cooperation mechanism for personal data protection facilitates the cross-border transfer of data by minimizing various regulatory and legal barriers, particularly in the e-commerce sector, thereby promoting fair competition in the global market.

C. COOPERATION AND CAPACITY-BUILDING MECHANISMS IN ICESCO MEMBER STATES

Recognizing the benefits of international cooperation in protecting personal data, it is essential to establish mechanisms and an institutional framework to enhance collaboration among ICESCO Member States. The following guidelines and approaches should be considered:

- Establishing regional networks for ICESCO Member States and exploring personal data protection issues with other countries. This initiative will foster collaboration among data protection bodies, governments, businesses, and civil society organizations, enabling the exchange of experiences, best practices, and resources. These networks will be designed to respect and leverage the cultural, linguistic, and geographical similarities of ICESCO Member States;
- Building bilateral or multilateral cooperation agreements among data protection bodies on both regional and inter-regional levels to facilitate information exchange, responses to notifications and alerts, and investigations of data security incidents to take appropriate measures. Moreover, such cooperation will support the adoption of common standards and best practices, promoting regulatory convergence and guiding organizations and businesses toward compliance;
- Creating a hub, forum or council of regional networks with a global and strategic mission of harmonizing regulations among different regions and countries and adopting common standards and best practices for the protection of personal data in all ICESCO Member States while taking into account the previous or future memberships of Member States in other global networks and groupings.

The establishment of an institutional mechanism for cooperation among ICESCO Member States will be key in building the capacity of personal data protection bodies by providing a framework for the implementation of specialized training and human resources support to help them address emerging data protection challenges, such as digital data security, privacy protection and regulatory compliance. In addition, cooperation mechanisms will foster public awareness and education on the multiple issues of personal data protection and the privacy rights of individuals in order to build and promote confidence in the use of digital technologies.

6 “CONCLUSION”

Protecting personal data has become a fundamental aspect of human rights in an increasingly digital world. This guide provides an introductory overview of the principles, best practices, and key regulations in personal data protection and explores the current state of personal data protection in ICESCO Member States and beyond.

It also highlights the importance of digital education in protecting personal data and privacy, offering consult, best practices, and specific recommendations. The guide aims to remind individuals of the need to comply with data protection standards and requirements. By raising awareness of potential risks and encouraging proactive measures, it seeks to foster a safer, healthier, more inclusive, and privacy-friendly digital environment for everyone. Additionally, it emphasizes the significance of establishing international cooperation mechanisms among ICESCO Member States, with a focus on lifelong learning to tackle data protection challenges. Ultimately, this guide serves as the initial resource for developing educational tools and materials to strengthen the capacities of decision-makers, users, and professionals alike.

7 GLOSSARY OF TERMS

Personal data : Information that directly or indirectly identifies an individual.

Data processing: Any operation involving data, i.e., collection, recording, organization, storage, adaptation, modification, extraction, search, use, communication, dissemination, limitation, destruction, etc., in accordance with the law.

Data Protection Authority: An independent government body in charge of monitoring compliance with laws and regulations on the protection of personal data.

Data portability: A person's right to retrieve and transfer their personal data from one service to another.

Consent: An individual's explicit or implicit agreement to the processing of their personal data.

Informed Consent: Consent given by an individual after being fully informed about the process and consequences of their data being processed.

Data Controller: A person or organization that determines the purposes and means of processing personal data.

Subcontractor: A person or organization that processes personal data on behalf of a data controller.

Right to be Forgotten: The right of individuals to request the deletion of their personal data, especially when it is no longer needed for the purposes for which it was collected or processed.

Image Rights: The right of individuals to control how their image is used and distributed.

GLOSSARY OF TERMS

Profiling: Using personal data to evaluate certain aspects of a person, such as their preferences, interests, health, economic situation, reliability, or to predict their behavior.

Transfer of Data Abroad: Moving personal data from one country to another or an international organization.

Data Breach: Unauthorized access, disclosure, alteration, or destruction of personal data.

Anonymization: the process of removing personal identifiers, both direct and indirect, that may lead to an individual being identified

Data Enciphering: Transforming data into an unreadable format that can only be accessed or decrypted by a user with the correct encryption key

Data Encryption: Using a computer program to transform data into a format that is unreadable by third parties, except for those who possess the decryption key.

Artificial Intelligence: Algorithms and mathematical models used to create systems that can learn, think, and make decisions based on data.

Internet-connected Object: A physical device with network communication capabilities, allowing it to interact, send, and receive data via the Internet.

Metaverse: An immersive virtual world in which users can interact and communicate with each other and the surrounding virtual environment in real-time.

8 USEFUL LINKS

https://www.dataguidance.com/laws

https://cybersecuritymag.africa/etats-des-lieux-des-legislations-sur-protection-donnees-personnelles-afrique

https://paradigmhq.org/wp-content/uploads/2021/09/DPA-Report-French.pdf

https://www.dlapiperdataprotection.com/index.html?t=law&c=SA

https://paradigmhq.org/wp- content/uploads/2023/07/Londa-2022-Gambia-Eng.pdf

https://www.dataguidance.com/opinion/brunei-darussalam-new-data-protection-regime-focus

https://help.openai.com/en/

JOIN US ! انضموا إلينا REJOIGNEZ-NOUS